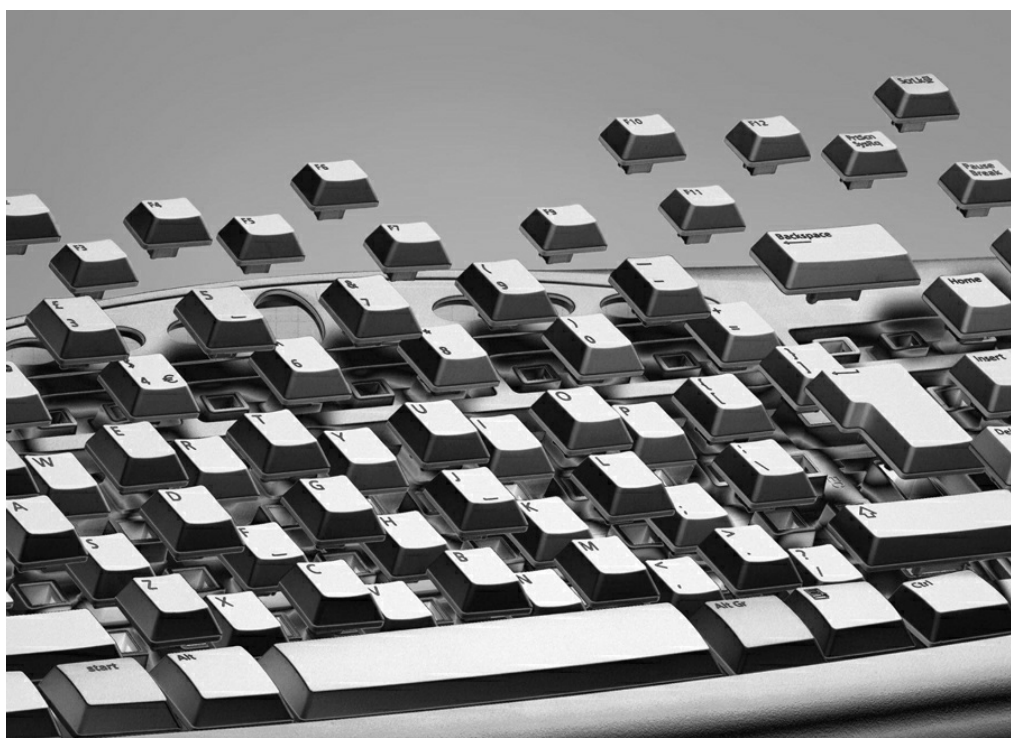


KINGPIN

HOW ONE HACKER TOOK OVER THE BILLION DOLLAR CYBER CRIME UNDERGROUND

KEVIN POULSEN
Senior Editor, Wired.com

Пролог

Такси стояло у порога небольшого магазинчика в даунтауне Сан-Франциско, пока Макс расплачивался с водителем и извлекал свою двухметровую тушу с заднего сиденья автомобиля, его густые тёмные волосы были собраны в гладкий хвост за затылке. Он вошел в магазин и подождал, пока машина, привезшая его, не уехала вниз по улице, прежде чем он решился проделать путь до своего убежища, расположенного в двух кварталах отсюда.

Мелкие магазинчики, новостные стойки и киоски, окружавшие его, пробуждались под рассветным небом, офисный планктон сползался в бизнес-центры, возвышавшиеся над ним. Макс тоже собирался работать, и его работа не оставляла ему ни малейшего шанса остаться дома после девяти для здорового полноценного сна. Последние несколько дней он провел в полном уединении. Стоило ему воплотить свой план в жизнь, и он понял, что пути домой не будет. Не будет возможности сбегать куда-нибудь перекусить в обеденное время. Не будет ночных посиделок у мультиплекса. Не будет ничего, пока он не закончит начатое.

Это был день объявления войны. Длительная прогулка по улице, вдоль которой толпились дома с одинаковыми оконными проёмами и отделкой цвета Голден Гейт Бридж, привела его к Пост Стрит Тауэрс. В течение нескольких месяцев он приходил в этот квартирный комплекс, делая все возможное, чтобы не выделяться из толпы иностранных студентов, привлечённых сюда возможностью снять жильё на короткие сроки по разумным ценам. Никто не знал его имени — во всяком случае, настоящего. И никто не знал его прошлого.

Здесь он был не Максом Батлером, смутьяном из небольшого городка, одержимым ломающим жизни насилием, и он не был Максом, самопровозглашенным компьютерным экспертом, которому платили 100 долларов в час за укрепление безопасности сетей компаний Кремниевой долины. Поднимаясь в лифте жилого дома, Макс становился кем-то другим: «Iceman`ом» — восходящим лидером криминальной экономики, ответственным за миллиарды долларов, украденных у американских компаний и их клиентов.

И Iceman был сыт по горло. Месяцами он «имел» продавцов по всей стране, получая кучи номеров кредиток, которые могли стоить сотни тысяч долларов на черном рынке. Но рынок был разрушен. Два года назад агенты секретных служб проехались виртуальным бульдозером сквозь главное место сбора компьютерного подполья, арестовывая главарей под дулом пистолета, и отправляя остальных

суетиться в чатах и маленьких веб-форумах, пронизанных дырами в безопасности и кишащих агентами спецслужб и стукачами. Это был полнейший хаос.

Знали они того или нет, но подполью нужен был сильный лидер, чтобы объединить всех. Чтобы навести порядок.

Выйдя из лифта и украдкой заглянув в коридор, чтобы проверить, нет ли кого на хвосте, Макс зашел в свою квартиру и слился с угнетающей духотой арендованной студии. Жара была самой большой проблемой этого места. Она знойной волной исходила от серверов и ноутбуков, втиснутых в любое сколь-нибудь свободное пространство. Как-то летом Макс принес туда несколько вентиляторов, но они помогли не сильно и настолько взвинтили счета за электричество, что хозяин квартиры начал подозревать его в выращивании травки. Однако это были всего лишь машины, вплетенные в одну большую сеть проводами, самые значимые из которых тянулись к гигантской параболической антенне, высунутой из окна, как снайперская винтовка.

Не обращая внимания на все неудобства, Макс сел за клавиатуру и принялся мониторить те сайты, на которых собирались киберпреступники — виртуальные площадки вроде Darkmarket или TalkCash. Два дня, что он занимался хакерством, его пальцы летали над клавиатурой с невероятной скоростью: он взламывал защиту сайтов, воровал их контент, логины, пароли и адреса электронной почты. Когда он уставал, он падал на складную кровать в своей комнате на час-другой, и затем с замутнённым взглядом опять возвращался к работе.

Несколько заключительных ударов по кнопкам клавиатуры, совершённые с той лёгкостью, с которой факир зажигает спичку, уничтожили базы данных сайтов. 16 августа 2006 года он слил беспрецедентное количество электронных адресов пользователям сайтов, которые он взломал: теперь все они были участниками CardersMarket.com, принадлежащего Iceman`у и внезапно ставшего самым большим криминальным рынком в мире, насчитывающим 6 тысяч пользователей и являющимся самым лучшим в своём роде.

Одним выстрелом Макс убил двух зайцев: подорвал годы усердной работы правоохранительных органов и воскресил преступное подполье, в чьих руках были сосредоточены миллиарды долларов.

Во всей России, Украине, Турции и Великобритании, в каждом доме, в каждом офисе, в каждой квартире Америки преступники были ошеломлены известием об этом первом враждебном захвате, произошедшем в подпольном мире. Некоторые из них держали в тумбочках оружие, чтобы защитить свои награбленные миллионы, но они не смогли сделать это. ФБР и агенты Секретной Службы США, потратившие

месяцы или даже годы на проникновение в ныне развалившиеся подпольные форумы, с равным ужасом читали сообщение, и на минуту все они: виртуозы хакинга, головорезы русской мафии, мастера поддельных удостоверений и полицейские, поклявшиеся ловить их — были объединены одной мыслью.

Кто такой *Iceman*?

Глава 1. «Ключ»

Как только пикап вкатился во двор, подростки-гики, сидевшие на корточках, поняли, что быть беде. «Чертовы слабаки!» — крикнул им из окна пикапа один из «ковбоев». Пивная бутылка вылетела из машины и разбилась о тротуар. Гики, вышедшие из клуба, чтобы поговорить вдали от громкой музыки и шума толпы, уже знали, что будет дальше. В Бойсе в 1988 году появиться на публике без ремня с широкой пряжкой и ковбойской шляпы означало совершить своего рода преступление.

Затем один из гиков сделал то, чего не ожидал ни один из «ковбоев»: он поднялся. Высокий и широкоплечий, Макс Батлер производил весьма внушительное впечатление; его причёска, острый трёхдюймовый панковский ирокез, увеличивала и без того немалый рост парня. «Слабаки?» — спокойно спросил Макс, прикидываясь, будто он не знает сленга, на котором говорили в Бойсе фанаты Новой волны и других музыкальных течений. «Что за хрень?» — двое «ковбоев» разразились ругательствами и уехали на скрипящем покрышками пикапе, размахивая резиновыми брызговиками.

Когда они встретились в средней школе, Макс стал неофициальным телохранителем сборища гиков в Меридиане, штат Айдахо, спальном городке, отделённом от Бойса восемью милями разномастных фермерских хозяйств. Век назад отцы-основатели Меридиана дали ему это имя за расположение точно на меридиане Бойса, одной из 37 невидимых и незаметных линий, пересекающих по вертикали карту Северной Америки. Но, возможно, единственная странность этого городка заключалась в том, что его школьная команда по скачкам состояла из одних девчонок.

Родители Макса женились молодыми, и они переехали в Айдахо из Финикса, когда он был младенцем. До некоторой степени Макс объединил их высшие качества: Роберт Батлер был ветеран Вьетнамской войны и увлечённым технологом, управлявшим компьютерным магазином в Бойсе. Натали Скорупски была дочерью украинских иммигрантов — она была гуманистом и сторонником мира, она любила расслабляться у Погодного Канала и смотреть документальные фильмы о природе.

Макс унаследовал ценности его матери, сторонясь красного мяса, сигарет, алкоголя и наркотиков, кроме злополучного эксперимента с жевательным табаком. От его отца Макс приобрел глубокую страсть к компьютерам. Он рос окруженным экзотическими машинами начиная с гигантских деловых компьютеров, которые мог

заменить офисный стол, заканчивая «портативными компьютерами» размером с чемодан от IBM. Максу было позволено играть с ними свободно. Он начал изучать основы программирования в возрасте восьми лет.

Но душевное равновесие Макса было нарушено: в возрасте четырнадцати лет он пережил развод родителей. Отец перебрался в Бойс, а Макс со своей матерью и младшей сестрой Лизой остался жить в Меридиане. Развод угнетающе подействовал на подростка, и, казалось, с тех пор он мог переключаться только между двумя «режимами работы»: расслабленность и полное безумие. Когда маниакальная сторона его личности разгоралась, мир становился слишком медленным, чтобы удержать его. Когда он получил водительские права, он принялся водить свой серебристый Ниссан с такой скоростью, словно педаль акселератора была обычным тумблером; он гонял от светофора до светофора, похожий в своих лабораторных очках на сумасшедшего учёного, проводящего эксперименты в области ньютоновской физики.

Поскольку Макс защищал своих друзей, они пытались защитить Макса от самого себя. Его лучший приятель, вундеркинд по имени Тим Спенсер, находил мир Макса увлекательным, но постоянно обуздывал порывистость своего друга. Однажды он вышел из своего дома и увидел Макса, стоящего у тщательно продуманной геометрической фигуры, горящей на газоне. Макс надыбал канистру бензина. «Макс, это наш дом!» — кричал Тим. Макс тихо извинялся перед Тимом, пока они затаптывали пламя.

• • •

Именно из-за его импульсивности друзья не стали говорить Максу о находке. Меридианские гики обнаружили связку ключей в незапертом столе у дальней стены химической лаборатории. Они выждали какое-то время, потом аккуратно выдвинули ящик, с опаской озираясь по сторонам, когда лаборанта не было поблизости. Они вытащили ключи, вынесли их из лаборатории и начали осторожно проверять на каждом замке меридианского кампуса. Так они выяснили, что один из ключей являлся главным: он открывал входную дверь и все последующие за ней двери.

Они сделали четыре его копии, по одной для каждого: Тима, Сета, Люка и Джона. Связку они вернули в темноту химической лаборатории после того, как тщательно стерли с нее все отпечатки. Общее решение было таково: Макс не должен ни о чем узнать. Главный ключ от старшей школы стал неким талисманом, с которым нужно было уметь обращаться с большой осторожностью, а не с расточительством и глупостью. Ребята поклялись сберечь его для какой-нибудь эпичной шутки на выпускном. Они могли бы, например, прокрасться в школу и хакнуть систему

громкоговорителей, чтобы в каждом кабинете зазвучала музыка. А пока ключ будет спрятан, и им вчетвером предстоит хранить этот большой секрет ото всех.

Никто не любил хранить секреты от Макса, однако они могли заметить, что у него уже были терки со школьной администрацией. Он откровенно смеялся над учебной программой, и, пока учителя талдычили про историю или решение всяких уравнений, Макс сидел, пролистывая распечатки с dial-up BBS (предшественником глобального интернета). Его любимым чтением была онлайновая хакерская брошюрка «Phrack» — творение хакерской сцены 80-х.

Первое поколение, достигшее совершеннолетия в эпоху домашних компьютеров, почувствовало всю мощь на кончиках своих пальцев, и Phrack был толчком революционной электрической информации из далекого мира, за пределами тихих границ Меридиана. Типичные статьи включали в себя обучающие программы о сетях с пакетной коммутацией, таких как Telenet и Tymnet, справочники по компьютерам телефонных компаний, как COSMOS, и вид изнутри крупномасштабных операционных системы, приводящих в действие универсальные ЭВМ и миникомпьютеры в кондиционируемых помещениях по всему миру.

Phrack также усердно отслеживал новостные репортажи с границ поля битвы между хакерами и их оппонентами, представляющими государственные и уголовные законы, которые только начинали справляться с проблемами, созданными развлекающимися взломщиками. В июле 1989 Корнелл — аспирант по имени Роберт Т. Моррис младший — был обвинён в соответствии с совершенно новым федеральным законом о компьютерном преступлении после того, как загрузил первого интернет-червя — вируса, заразившего шесть тысяч компьютеров, забивавшего пропускную сетевую полосу и ведущего систему к остановке. В этом же году в Калифорнии молодой Кевин Митник заработал свой второй хакерский арест и получил один год тюремного заключения — поразительно суровый приговор для того времени.

Макс стал «Господином Максом» на электронных досках объявлений Бойса и вникал в телефонный фрикинг – хакерскую традицию уходящую корнями в 70ые. Когда он использовал модем на своем Commodore 64 для сканирования свободных междугородних кодов, он впервые столкнулся с федеральным правительством: агент секретной службы из местного отделения навестил Макса в школе с доказательствами фрикинга. Поскольку он был несовершеннолетний он избежал серьезного наказания. Но агент предупредил Макса, чтобы он сменил курс пока он не попал в настоящую беду.

Макс пообещал, что он усвоил урок. Затем случилось немыслимое. Макс заметил странную форму на связке ключей Джона и спросил что это. Джону пришлось

признаться.

В тот же вечер Макс и Джон вошли в школу и устроили погром. Один или они вдвоем исцарапали надписями стены, распылили огнетушители по коридорам и ограбили закрытый шкаф в химической лаборатории. Макс утащил кучу химикатов и закинул их на заднее сидение своего автомобиля. Ранним утром Телефон Сэта зазвонил. Это был Макс. Он оставил Сэту подарок во дворе. Сэт вышел и обнаружил бутылки с химикатами на своей лужайке. В панике он сгреб их, перенес на задний двор, где схватил лопату и стал копать яму.

Его мать вышла на задний двор и застала там Сета, пытающегося уничтожить улики. «Ты же понимаешь, что я обязана сообщить об этом в школу?» — спросила она. Сета отвели в кабинет директора и допросили, однако он наотрез отказался выдать Макса. Все компьютерщики Старшей школы Меридиана по очереди были приведены на допрос офицером школьной службы безопасности; некоторых из них вели в наручниках. Когда настала очередь Джона, он не выдержал и раскололся. В школу вызвали полицию, которая обнаружила предательские жёлтые пятна йода на заднем сидении Ниссана, принадлежавшего Максу.

Кража химических реактивов в Меридиане каралась очень строго. Макса исключили из школы и привлекли к уголовной ответственности как несовершеннолетнего. Его обвинили в умышленном причинении вреда имуществу и тщательно спланированной краже без каких-либо смягчающих обстоятельств. Затем его отправили в клинику на две недели для проведения судебно-психологической экспертизы, в результате которой ему был поставлен диагноз — биполярное расстройство.

Максу был вынесен приговор – условное наказание. Мать отправила его в Бойс к отцу и определила его в Бишоп Келли, единственную в штате католическую старшую школу. Мера наказания, назначенная Максу, была очень мягкой. Но это сильно повлияло на характер: он стал более импульсивным и непослушным. Макс решил, что ему нужно гораздо больше отмычек.

Глава 2. «Смертельное оружие»

Это комната развлечений!!!

Комната развлечений представляет из себя большое затемнённое помещение без четкого выхода. Публика может расслабляться на подушках перед гигантским экраном телевизора. В наличии имеется также набитый доверху холодильник и бар.

Эта надпись приветствует посетителей TinyMUD, игрового виртуального мира, который был внутри компьютера размером с мини-холодильник на полу в офисе Питтсбургской аспирантуры. В 1990 года сотни студентов по всему земному шару «выходили в люди» или социализировались через Интернет. Макс, первокурсник университета штата Айдахо в Бойсе был одним из них.

Интернет на тот момент существовал уже 7 лет, и около 3 миллионов людей имели доступ через жалкие триста тысяч хостов оборонных предприятий, секретных военных объектов и небольшого числа устройств, установленных в колледжах и университетах. В академических кругах Интернет казался сложным для использования непосредственно студентами. Но случилось то, что позволило любому уважающему себя американскому колледжу или институту активно пользоваться Интернетом. MUD‘s — многопользовательские миры — стали любимой Интернет-тусовкой тогдашней молодёжи.

Mud был чисто текстовым «опытом», как и всё в мире довебовского Интернета. Масштаб игры полностью определялся написанным текстом, и перемещаться в ней можно было с помощью простых команд, таких как «север» и «юг». Существовала и более современная версия обычного Mud‘a — TinyMud, коренным образом отличавшаяся от остальных. Это была первая многопользовательская игра, откуда разработчики выкинули файлы «Подземелья и Драконы». На работе этих пресловутых файлов основывался игровой процесс предыдущих Mud`ов. В TinyMud активные пользователи создавали и изменяли собственный игровой мир, не прибегая к услугам администраторов и «мудрецов». Любой желающий мог сотворить целую Вселенную вокруг своего персонажа с собственными атрибутами, границами, а также приглашать туда гостей. Жителей TinyMud быстренько превратили «комнату развлечений» в мировой социальный киберцентр. Вход и выход были синхронизированы с такими локациями, как Волшебный Дворец Искажения, квартира Гоундархла и сотнями других.

Также наследием от TinyMud стала система вознаграждения в стиле D&D. Особое

значение придавалось поискам сокровищ, конечным квестам и качу. Поэтому вместо того, чтобы тратить время на банальные сражения с орками и накопление очков, пользователи разговаривали, флиртовали, сражались и даже занимались виртуальным сексом. Но стоило только освободить игру от ограничений Толкиеновской ролевухи, как она превратилась во «вторую жизнь» для многих пользователей. Сила зависимости от игры возросла в геометрической прогрессии. В то время распространённой шуткой была расшифровка аббревиатуры Mud как Multi Undergraduate Destroyer (Всесторонний Студенческий Деградант). Для Макса это было больше, чем просто шутка.

По настоянию Макса его девушка Эми добавилась на один из TinyMud`ов. Оригинальная версия этого TinyMud была в Университете Карнеги-Меллон, но к тому времени такой же софт содержали другие Мады, разбросанные по всему Интернету. Макс стал «Лордом Максом», а Эми взяла имя героини из книги «Элрик из Мелнибонэ» и коротких рассказов Майкла Муркока, — Киморил.

Киморил была возлюбленной Элрика, слабого задохлика — альбиноса. Впоследствии Элрик стал внушающим страх императором, который использовал волшебную силу меча Стормбрингер. Для Макса же волшебный меч был метафорой, означавшей то, что компьютер в умелых руках может сделать из обычного человека короля. Но вот для Элрика Стормбрингер был также и проклятьем. Меч был мистическим образом связан с его обладателем. Попытка избавиться от меча ни к чему не привела. Элрик пронёс «проклятый» меч через всю жизнь.

По книге роман Элрика и Киморил был обречён. Девушка погибла во время штурма родного города Элрика Имрирра пиратами. Главой пиратов был Йиркун, враг Элрика и по совместительству его двоюродный брат. Но, тем не менее, для Макса эта история стала идеалом романтической любви, особенно после развода его родителей. Киморил умоляла Элрика вложить Стормбрингер в ножны и прекратить сражение, но Элрик в гневе нанёс Йиркуну смертельный удар, поддавшись чарам своего меча. Умирая, Йиркун толкнул любимую Элрика на остриё Буреносца, лишив Императора счастья. Тем самым Йиркун был отомщён.

> Жуткая правда открылась Элрику, и он издал животный крик отчаяния. Любимая девушка погибла по его вине. Меч, разукрашенный рунами и запятнанный кровью Киморил, выпал из его руки и камнем полетел вниз. Рыдая, император упал рядом с телом своей любимой и взял её за руки.
>
> «Киморил,- стонал он, дрожа всем телом — Киморил, я убил тебя!»

Когда Эми первый раз встретила Макса, то решила, что он крутой бунтарь и немного панк. В нём не было ни капли от офисного планктона и, как ни странно, от толпы в городе Бойсе. Но, проводя с Максом всё больше и больше свободного времени, она увидела более тёмную одержимую сторону его характера, особенно после того, как Макс познакомил её с Интернетом и TinyMud.

Первое время Макс был в восторге от того, что девушка разделила с ним его страсть к онлайн мирам. Но как только Эми стала заводить новых друзей на своей учётке в Mud (в том числе и мужского пола), Макс стал ревнивым и агрессивным. Для него не было разницы, изменяет ли ему Эми в реальной жизни или в виртуальной: измена была налицо. И он теперь он уже пытался её заставить не заходить в TinyMud. Эми отказывалась, и пара начала ссорить как онлайн, так и в жизни.

В конце концов Эми «достало» то, что они ругались из — за какой — то компьютерной игры. В ранний октябрьский вечер 1990 года, в среду, когда Макс и Эми находились в разных игровых комнатах на TinyMud, Киморил наконец — то сказала своему Лорду Максу, что не уверена в продолжении их дальнейших отношений.

Эта была первая серьёзная связь Макса, поэтому ответная реакция была сильной. Они же поклялись быть вместе всю жизнь, и «лучше было бы умереть, чем жить друг без друга», — написал Макс в TinyMud. Затем он в красках «объяснил» Эми, как бы он её уничтожил. Другие пользователи с обеспокоенностью наблюдали, как неистовство Макса принимало характер реальной угрозы. Что им следовало бы предпринять?

Один из «мудрецов» TinyMud пробил IP-адрес Макса и выяснил, что он принадлежит Университету штата Айдахо в Бойсе. Mud`еры нашли телефон Департамента Шерифа округа Ада в Бойсе и позвонили туда с предупреждением о возможном убийстве-суициде.

Год начался для Макса удачно… Его отец, владелец компьютерного магазина HiTech Systems, всегда давал ему какую-то работу. Макс отлично преуспевал, выполняя канцелярские обязанности, делая доставки на фургоне компании и собирая PC-совместимые компьютеры в магазине. Он не нарушал режим пробации (испытательный срок) и даже перестал принимать лекарства от биполярного расстройства, так как был не согласен с диагнозом. Кроме того, отец Макса не хотел, чтобы сын стал наркоманом или получил лекарственную зависимость.

Он начал встречаться с Эми в феврале 1990 года, через 4 месяца после встречи с ней «Зоопарке», танцевальном клубе в Бойсе, который был ориентирован на

подростковую публику. Эми была очаровательной блондинкой с голубыми глазами и моложе Макса на год. Он познакомился с ней с подачи своего друга Люка Шенемана, одного из вахтёров Меридианской школы. Как только Макс закончил школу, отношения с Эми стали более серьёзными.

Макс обычной доводил всё до логического конца и был полностью предан Эми. Она планировала поступить в Университет штата Айдахо в Бойсе, и это обстоятельство заставило Макса отложить своё собственное поступление в такие крутые учебные заведения, как Массачусетский Технологический институт или Университет Карнеги-Меллон. Он приводил Эми домой, чтобы она увидела его крутой комп и сыграла с ним на пару в Тетрис. Их отношения отличались от того, что когда-то было у родителей. Ребята думали, что эта романтика никогда не кончится.

Макс почти не встречался с друзьями во время летних каникул. В конце августа начались занятия в Университете штат Айдахо. При поступлении Макс сразу же выбрал факультет и специальность. И, как вы догадались, это была Информатика. Он был зачислен на следующие курсы: математический анализ, химия и занятия, связанные со структурированием различных данных на компьютере. Как и всем студентам, ему была выделена своя учётка в системе UNIX. Макс был немногим из тех, кто решил сразу же проверить на прочность эту компьютерную систему. Наряду с Максом, другой студент, Дэвид, уже взламывал аккаунты преподавательского состава. Они проводили часы в серверной комнате университета, уставившись в висящий зелёный текст терминалов и стуча по звонкой клавиатуре. Они буквально «летали» по почтовым ящикам преподавателей, отправляя от их имени сообщения или отвечая на них. При этом Макс и Дэвид были настолько поглощены процессом, что редко прерывались на разговоры друг с другом. Дэвида раздражала в Максе неспособность доводить какое-либо дело до логического завершения, а также очень медленная скорость набора текста. Макс чувствовал это и постоянно огрызался. «Чего ты ждёшь?» — говорил Макс, когда Дэвид без причины замолкал. «Ответной реакции», — ухмылялся тот.

Администрация университета в общем могла перенести один какой-нибудь мелкий взлом, но когда Макс начал взламывать другие Интернет — системы, то ему официально закрыли доступ ко всем университетским компьютерам. Но вскоре доступ был восстановлен, но Макс опять вернулся к TinyMud и конфликту с Эми…

Тогда-то шериф и позвонил университетскому системному администратору в 2 часа ночи, чтобы предупредить об угрозе двойного убийства. Полиции были необходимы копии компьютерных файлов Макса в качестве улик. Просьба такого рода означала немало проблем для репутации университета. После консультации с адвокатом администрация решила добровольно ничего полиции не передавать. Они

предпочли сохранить файлы Макса на перфоленте и отстранить «героя» от компа.

Что касается Эми, то она всё ещё беспокоилась о Максе, хотя уже начинала продумывать процесс расставания с ним. В её душе ещё тлели чувства к Максу, и она боялась, что он может необдуманно себе навредить.

Макс продолжал звонить после TinyMud'овского инцидента. Их разговор всегда проходил по одному и тому же сценарию. В начале тон Макса был дружелюбным. Начиная разговор в дружелюбном тоне, Макс как бы показывал свою светлую сторону, так хорошо знакомую его друзьям и родственникам. Затем он переходил к жалости к себе любимому и угрозам, становясь бешеным в конце разговора.

30 октября Макс сказал Эми, что хотел бы поговорить с ней наедине. Не ожидая ничего плохого и ещё надеясь закончить отношения с Максом мирным путём, Эми согласилась на встречу (тем более, она не раз видела Макса в университетском городке). Макс вернулся в дом своей матери в стиле ранчо, который находился на тихой улочке в Меридиане, в квартале от его старой школы.

Он встретил Эми в дверях и пригласил в спальню в задней части дома, уверяя, что не сделает ничего дурного. Матери дома не было, а его 14-летняя сестра смотрела телевизор.

Они расположились на матрасе, который валялся на полу, и стали обсуждать свои чувства. Эми призналась, что уже встретила другого парня в TinyMud. Он жил в Северной Каролине и его звали Чад. Их отношения уже вышли за пределы клавиатуры, и молодые люди отправляли друг другу фотографии по e-mail, а также активно общались по телефону.

Макс пытался контролировать себя, с трудом сдерживая слёзы. Он почувствовал, что его предали, и не мог поверить в то, что только что услышал. Макс взял у Эми номер Чада и позвонил своему онлайн сопернику при помощи междугородней телефонной карты.

Далее в разговоре участвовали три человека: Макс представился Чаду и затем позволил Эми взять трубку. Она сказала Чаду о своих чувствах. Затем Чад позвонил на телефон Макса и начал болтать с Эми.

Макс окончательно взбесился — схватил трубку и повесил её. Эми внимательно наблюдала за участившимся дыханием Макса и его бегающими глазами.

— Я убью тебя, — заорал он — Ты умрёшь прямо сейчас.

Она ответила, что не чувствует себя предательницей и не будет извиняться. Он повалил её на матрас и попытался задушить.

— OK, — сказала она — Почему же ты меня не убиваешь?

К счастью, Макс начал контролировать себя и потребовал, чтобы Эми убралась из его дома. Он вышвырнул её за дверь со словами: «Проваливай отсюда! Я не хочу убивать себя… Но имей ввиду, что я ещё могу изменить своё решение». Эми запрыгнула в свою машину и исчезла за считанные секунды.

На обратном пути она всё прокручивала в голове последние события. Теряясь в своих мыслях, она не замечала других машин, пока с треском не влетела в одну из них. Противостояние двух металлических конструкций закончилось зловещим хрустом. Обе машины были повреждены, но несерьёзно. Когда же родители Эми узнали о происшествии в доме Макса, она начали беспокоиться за жизнь своей девочки. Через неделю после аварии, Эми пошла в полицию, и Макс был арестован.

Позже Макс рассказывал своим друзьям, что Эми немного преувеличила в оценке ситуации. В её версии Макс удерживал девушку в заложниках в спальне долгое время и неоднократно душил. По версии Макса он держал руки на её горле но не душил, и Эми могла выйти в любой момент. Эми сказала, что Макс продолжал одержимо названивать ей после аварии и угрожать. Макс отвечал, что вообще не видел и не слышал эту ненормальную после того, как выкинул её из квартиры. В отличие от Макса, который действительно страдал из-за этой ситуации, Эми использовала данный случай, чтобы выпутаться из неприятностей, связанных с аварией.

Окружной прокурор предложил Максу сделку с правосудием согласно его проступку. Но месяц назад ему было объявлено, что он может получить всего 45 дней или вовсе быть отпущенным под залог. И Макс, будучи свободным, случайно встретил Эми, которая прогуливалась за ручку с своим новым парнем по университетской аллее. И вновь эмоции Макса заслонили его разум. В горячке он припарковал грузовик отца на лужайке и пошёл навстречу парочке. Его всего трясло.

— Привет, — сказал он.

— Ты не имеешь права видеться со мной, — ответила Эми.

— А ты не помнишь, что между нами раньше было? — парировал Макс.

Спутник Эми попытался вмешаться, но Макс предупредил его: «Лучше позаботься о себе, друг!» Затем он удалился в сторону машины. Вскоре взревел двигатель грузовика, и машина стала быстро приближаться к любовной парочке на тротуаре. Мощный поток воздуха от движущейся махины чуть не снёс Эми. Ещё секунда, и влюблённых не было бы в живых.

Сделка с правосудием была нарушена. Окружной прокурор по закону упёк Макса за решётку, обвинив его в «нападении с применением смертельного оружия — рук». Это обвинение было сомнительным. Руки Макса были опасны не более, чем руки любого другого человека.

Сторона обвинения предложила ему девять месяцев тюрьмы в обмен на признание в том, что он душил Эми. Естественно, Макс отказался. После трёхдневного судебного разбирательства и полуторачасового совещания судья признал его виновным по отношению к Эми. 13 мая 1991 года Тим Спенсер и ещё пара выпускников Меридианской старшей школы находились в суде и наблюдали за тем, как судья Дебора Бейл без малейшей жалости приговорила их друга к 5 годам тюрьмы.

Глава 3. «Голодные программисты»

Макс нашёл дом Тима Спенсера на вершине одного из холмов, отделяющих полуостров Сан-Франциско от понатыканных по всему Тихоокеанскому побережью тихих и захолустных городишек. Но слово «дом» слабо подходило к описанию данного сооружения. Это была огромная вилла площадью 6000 квадратных футов на участке в 50 акров, откуда открывался прекрасный вид на город Халф Мун Бэй. Макс прошёл через главные ворота и парадные двери в просторную гостиную с красиво изогнутыми стеклянными стенами растянутыми от пола до потолка.

Он приехал в Сан-Франциско через год после условно-досрочного освобождения, чтобы начать всё сначала. Тим и его друзья из Айдахо, снимавшие этот дом, называли его «Голодный Дом». Это название напоминало им о первом совместном предприятии, начатом годом ранее. Они планировали приобщиться к индустрии Кремниевой Долины путём создания небольшой компьютерной фирмы под названием «Голодные Программисты», сотрудники которой работали буквально «за еду». Однако вскоре айтишники нашли своё место в компьютерном бизнесе и «Голодные Программисты» превратились в неофициальный клуб по интересам Тима и его друзей из Меридианской школы и Айдахского университета. Голодный Дом был основной базой клуба, где все развлекались. Кроме того, здесь жили пять его членов. Макс теперь будет шестым.

Он приехал в Голодный Дом с минимумом вещей и огромной тяжестью на сердце, так как судебная система несправедлива обошлась с ним. В 1993 году, когда Макс второй год сидел в тюрьме, Верховный Суд Айдахо вынес решение, что руки «или другие части тела и его придатки» не могут являться смертельным оружием. Это означало, что Макса осудили ни за что. Но несмотря на решение Верхового Суда, просьба о помиловании была отклонена. Судья признал, что Макс был формально не виновен в совершении тяжкого преступления, за которое «тянул срок», но адвокаты вовремя не подали иск, поэтому поезд ушёл.

Когда же Макса наконец-то освободили 26 апреля 1995 года, он осознал, что отсидел практически ни за что 4 года в тюрьме штата Айдахо, хотя его преступление «тянуло» дней на 60 в окружной тюрьме. В то время, когда он сидел за решёткой, его друзья закончили колледж и получили достойное образование, позволившее им уехать из Айдахо и начать перспективную карьеру.

Макс приехал со своим отцом в Сиэтл, а Тим, Сет и Люк подкатили из Сан-Франциско на встречу выпускников — программистов из Меридианской школы. Друзья поразились крепкому телосложению Макса (Результат его упорных тренировок в тюрьме!) и его безудержному оптимизму, которому не мешало ни отсутствие диплома, ни уголовное прошлое. Макс знал, что пришло время безграничных возможностей: через три месяца после его осуждения британский учёный-программист создал Всемирную паутину. Сейчас там было около 19000 сайтов, в том числе и для Белого дома. Интернет-провайдеры всплывали в каждом уважающем себя городе, а крупные компании типа America Online и CompuServe добавили к своим предложениям услугу доступа к сети.

Интернет стал доступен широким слоям населения. А Макс из чудаковатого компьютерщика превратился в высококлассного специалиста, разбиравшегося в том, что быстро завладело миллионами людей. Благодаря своим знаниям Макс вполне мог бороться за вакансию it-специалиста в Сиэтле. И он боролся, делая акцент на вакансиях работников техподдержки, разбирающихся во всех тонкостях компьютера и компьютерных сетей.

Макс нашёл работу и теперь подолгу болтался в «неблагополучных» районах, разбираясь с «ужасными» компьютерами. Пытаясь найти необходимый кураж, он вернулся к ещё сохранившейся системе группового общения IRC. Когда Макса «упекли» за решётку, IRC был неимоверно популярен в тогдашнем обществе. Но с развитием и совершенствованием Интернета многие пользователи стали применять более простые способы обмена мгновенными сообщениями и веб-чаты. Те же, кто продолжал пользоваться IRC, были, как правило, либо чокнутыми гиками, либо хакерами — дилетантами, либо пиратами, проворачивающими через компьютеры свои грязные делишки где-то в забытых тоннелях и переулках.

До тюрьмы Макс активно пользовался IRC. Компьютерный гений представлял себя невидимкой в киберпространстве. Ему нравилась эта роль. Он выбрал псевдоним «Ghost23», так как число 23 было для него счастливым. Помимо всего прочего, по китайской Книге Перемен И-ЦЗИН гексаграмма под номером 23 предвещала крупные перемены в жизни, сеяла хаос. И Макс влился в пиратское сообщество с помощью IRC. Членам этого сообщества были люди, которые плевали на какие-либо законы об авторском праве, завоёвывали себе репутацию путём перекачивания музыки, игр и программного обеспечения. Там компьютерные навыки Макса нашли подходящее применение. Он обнаружил незащищённый файловый сервер (FTP) в Литлтоне, Колорадо и превратил его в кэш украденного программного обеспечения для него и его друзей и укомплектованный нелицензионными копиями таких программ, как NetXray, Laplink и Symantec pcAnywhere.

Но его увлечение пиратством сыграло с ним злую шутку. Провайдер обнаружил подозрительные загрузки на сервера корпоративных офисов компании CompuServe в Бельвю, где Макс только-только получил работу. И не надо было иметь семи пядей во лбу, чтобы понять: Макс «спалился». Дело получило широкую огласку. О Максе стали постепенно забывать только через год после его освобождения.

Как раз тогда Макс решил начать всё заново в Кремниевой долине, где доткомовская экономика разрасталась как снежный ком, и любой талантливый компьютерщик мог подобрать работу, не беспокоясь о своём прошлом. Максу нужно было новое, незапятнанное имя. Макс придумал себе новый псевдоним — «Макс Вижн». Этот позитивный псевдоним в полной мере отражал все стремления Макса. И как только наш герой увидел очертания Сиэтла в зеркале заднего вида своей машины, он сказал «Пока» Максу Батлеру. С сегодняшнего дня он стал Максом — Рентгеном (Max Ray Vision).

• • •

Дальновидный Макс понял, что жизнь в Хангри Мэнор просто замечательна. Со всех сторон окружённый холмистыми лугами дом мог похвастаться двумя флигелями, четырьмя спальнями, комнатой для прислуги, полноценной столовой, загоном для скота и кирпичной дровяной печью как в итальянской пиццерии, а также барбекюшницей, находившейся в вентилируемой комнате рядом с огромной светлой кухней. «Голодные» жители поместья превратили библиотеку в компьютерный класс и серверную комнату, заставленной множеством заказных игровых ПК для развлечений. Они проложили сетевой кабель для высокоскоростного Интернета в каждую комнату, для чего потребовалось частичное отключение электричества в районе 92 шоссе из-за трудностей с этим самым телефонным кабелем. Старинная телефонная система связывала западное крыло с восточным. В качестве «изюминки», один из «голодных» установил во дворе гидромассажную ванну, что позволяло вечером отдыхать после работы и наблюдать за звёздами.

Другой нашёл Максу работу в качестве системного администратора в MPath Interactive. Эта компания была знаменита тем, что давала немалые деньги для стартапа крутым геймерам Кремниевой Долины. Макс с головой окунулся в работу. Вопреки стереотипам компьютерного «ботана», ему нравилось не только устранять неполадки в работе компьютеров и исправлять ошибки, но и реально помогать людям. Наконец-то он обрёл тот долгожданный драйв, которого ему не хватало.

Но эта идиллия была нарушена неожиданным приветом из прошлого. Судебный курьер, явившийся как гром среди ясного неба, вручил Максу иск на 300,000$. Иск был подан Ассоциацией разработчиков программного обеспечения. Эта

промышленная организация решила использовать возможное поражение Макса в суде как предупреждение всем интернет-пиратам. Как провозгласила Ассоциация в пресс-релизе: «Эта акция является уроком для тех интернет-пользователей, которые считают, что могут нарушать авторские права, не опасаясь огласки или наказания».

Так как это был первый подобный иск, он сразу же получил огласку как в виде краткой, но информативной статьи в журнале Wired, так и в виде упоминания в слушаниях в Конгрессе по закону об интернет-пиратстве. Удивительно, но жизнь Макса нисколько не изменилась, даже после того, как его имя стало «притчей во языцех».

Когда волнения в прессе утихли, Ассоциация разработчик (SPA) была готова тихо «замять» дело за 3,500 $ и пару — тройку бесплатных компьютерных консультаций. Но существовала и обратная сторона медали — Макса заметили в ФБР.

Крис Бисон, молодой агент из Бюро по поимке киберпреступников доходчиво объяснил Максу его задачи. С помощью Макса ФБР планировало находить подпольных киберпреступников. Хакеры, занимающиеся пиратством и распространением нелицензионных версий игр и музыки, больше их не интересовали. Появились новые, более опасные «деятели» в криминальной компьютерной среде — «реальные» преступники. Они были настоящими киберворами, педофилами и даже террористами. «ФБР больше не гоняется за такими людьми, как ты, Макс», — сказал Бисон.

В марте 1997 Макс Вижн был формально введён в программу осведомителей ФБР. Его первым письменным отчётом для Бюро были: вводный курс по варезу и написанию вирусных программ; руководство по взлому компьютеров. Последующий отчёт касался файлообменников, один из которых он эксплуатировал в Сиэтле, и нелегального объединения Rabid Nevrosis. Это объединение уже успело наследить в прошлом октябре, выставив в открытый доступ пиратский релиз Металлики «Ride the Lightning».

Когда же Макс добрался до пиратской версии программы AutoCAD, то получил в награду от ФБР 200$. Макс подписал квитанцию агентурным именем Эквалайзер, как заставил Бисон. Как ни странно, эти двое пока мирно уживались друг с другом. Но никто из них ещё не знал, что Крис Бисон в будущем посадит своего Эквалайзера за решётку и превратит его в одного из тех неуловимых преступников, кого он так мечтал поймать.

Глава 4. «The White Hat»

Макс строил свою новую жизнь в период глубоких перемен в хакерском мире.

Первые люди, которые идентифицировали себя как хакеры, были студенты, которые осваивали программное обеспечение и электронику в MIT в 1960-е. Это были умные дети, принимавшие непочтительный, не авторитарный подход к технологии. Они завершают новаторско-неряшливый противовес joyless-suit и lab-jacket, как IBM. Пранкинг был частью хакерской культуры, и фрикинг туда же — по большей части нелегальное исследование забытых магистралей в телефонной сети. Но взлом был, прежде всего, творческим трудом, который привел к бесчисленным переломным моментам в истории компьютеров.

Слово «хакер» приобрело негативный окрас в начале 1980-х, когда первые домашние компьютеры — the Commodore 64s, TRS-80s, Apple — пришли в комнаты студентов на окраинах и городах во всех Соединенных Штатах. Эти машины были продуктами хакерской культуры: Apple II, а вместе с ним и сам концепт «домашний компьютер», зародилось благодаря двум фрикерам, которых звали Стив Возняк и Стив Джобс. Но не все подростки были обеспечены компьютерами, и многие с нетерпением ждали «взрослой жизни», чтобы ощутить всю в мощь процесса и исследования сетей, которые достигаются с помощью телефонного звонка или визга модема. Так они начали незаконные вылазки в корпоративные, государственные и академические системы и делали свои первые робкие шаги в ARPANET, предшественник Интернета.

Когда эти первые молодые злоумышленники начали терпеть неудачи в 1983 году, национальная пресса нашла слово, чтобы описать их, и они стали именоваться «Хакеры». Как и в предыдущем поколении хакеров, они раздвигали границы технологий и делали вещи, которые казались всем невозможными. Но не для них — пробивающих бреши в корпоративных компьютерах, захватывающих телефонные коммуникации и проскальзывающих в государственных системы, университеты и защищающих сети подрядчиков. Олдскульщики содрогнулись от такого сравнения, но с этого момента, слово «хакер» будет иметь два значения: талантливый программист, который подтянулся собственными силами, и компьютерный злоумышленник. Вдобавок к путанице, многие хакеры были и тем, и другим.

Теперь, в середине 1990-х, сообщество хакеров снова разделилось. ФБР и Секретная Служба инсценировали аресты громких злоумышленников, таких, как Кевин Митник и Марк «Phiber Optik» Абен, Нью-Йоркский телефонный взломщик,

и перспектива тюрьмы ставила крест на развлекательном вторжении, ставя риск намного выше удовлетворения собственного эго и приключений.

Теперь интернет был открыт для всех и персональные компьютеры стали достаточно мощными, чтобы запустить те же операционные системы и языки программирования, которыми до этого могли пользоваться только большие любители. И теперь в кибербезопасность потекли реальные деньги.

Взламывать системы становилось не круто. Те, кто обладал мышлением хакера, все чаще и чаще находили себе легальную работу. И злоумышленники вешали свои черные шляпы и переходили на светлую сторону. Они стали «Whitehat hackers», ссылаясь на героев из старых ковбойских фильмов, используя свои компьютерные таланты и навыки для защиты правды и справедливости.

Макс думал о себе, как о white hat. Отслеживание новых типов атак и уязвимостей стало его работой и как Max Vision, он начинает способствовать некоторым рассылкам по компьютерной безопасности, где обсуждались последние события. Но полностью изгнать из себя личность Ghost23 ему не удается. Это не было секретом среди друзей Макса, что он продолжает взламывать системы. Когда он встречал что-то новое или интересное, он не видел никакой опасности в том, чтобы забрать это себе.

Тим был на работе в тот день, когда позвонил сбитый с толку системный администратор из другой компании, отследивший проникновение в Hungry.com – онлайн-дом «Голодных Программистов», где они размещали проекты, вывешивали резюме, оставляли емэйл-адреса, которые сохранялись неизменными при смене работы или других эксцессах. На общем ресурсе были десятки гиков, но Тим знал, кто ответственен за проникновение. Он оставил сисадмина на другой линии и позвонил Максу.

«Прекрати взламывать. Сейчас же» — сказал он.

Макс пробормотал извинения. Тим переключился на линию с системным администратором и радостно сообщил, что нападение было остановлено.

Жалоба удивила и смутила Макса – если его цели знали, что он хороший парень, тогда и нет никаких проблем из-за безобидного проникновения. «Макс, ты должен получить разрешение» — пояснил Тим. Он дал ему жизненный совет. «Просто представь, что все смотрят на тебя. Это отличный способ убедиться, что ты делаешь все правильно. Если бы я стоял рядом или твой отец, чувствовал ли ты тоже самое, когда все это делал? Что бы мы сказали?»

Если и была вещь, которую Макс упустил в своей новой жизни, то это было бы

отсутствие партнера, с которым можно было поделиться. Он познакомился с 20-летней Кими Винтерс на рейве «Warmth», который проходил на заброшенном складе. Макс был главным на сцене, танцуя с удивительной грацией; он крутил руками как Бразильский танцор огня. Кими — студентка общественного колледжа и бариста на полставки, с ногами короче, чем у Макса. Она расхаживала в бесформенной черной толстовке унисекс, которую любила одевать при выходе в свет. Но если приглянуться, она была определенно очень милой, с щечками, как наливные яблочки и с кожей цвета меди как у ее корейской мамы.

Тусовки в «Голодном Доме» были легендарными и когда Кими появилась в гостиной она была заполнена десятками гостей из клавиатурной касты силиконовой долины – программистами, системными администраторами и веб-дизайнерами перемешанными под стеклянной люстрой. Макс засиял когда увидел её. Он провел для нее экскурсию по дому, указывая на атрибутику добавленную Голодными Программерами.

Экскурсия закончилась в спальне восточного крыла «Голодного Дома». При всем величии дома, комната Макса была как келья – никакой мебели, кроме футона (японский хлопчатобумажный матрац) на полу, никаких удобств за исключением компьютера. Для вечеринки Макс направил синий и красный прожекторы на бутылку мятного шнапса (это был единственный его порок). Следующим вечером Кими пришла на ужин, в вегетарианском меню которого, содержалось только одна позиция – сырое тесто. Макс порезал остатки печенья и подал со шнапсом. В конце концов, почему бы не съесть сырое тесто на ужин, раз нет других вариантов?

Кими была заинтригована. Максу нужно так мало для счастья. Он прям как ребенок. Когда вскоре после вечеринки наступил День рождения Макса, она послала ему в офис в MPath коробку украшенную шариками и Макс был тронут до слез таким жестом. Она была девушкой его мечты, как сказал он ей позже. Они начали думать о том, чтобы начать жить вместе. В сентябре, хозяин «Голодный Дом», недовольный владением особняка программистами, вернул себе его и после прощальной тусовки их общий дом рассеялся по всему Bay Area. Макс и Кимим осели в Маунтин-Вью, в тесной студии баракоподобного комплекса на 101-ом шоссе, перегруженной транспортной артерии Силиконовой Долины.

Макс возобновил свою работу на ФБР и его призрак IRC привел его к новой возможности – стать white hat. На одном из каналов он подружился с человеком, который в Сан-Франциско открыл консалтинг-фирму и был заинтересован в участии Макса. Макс поехал в город, чтобы нанести визит Мэтту Хэрригану, ака «Digital Jesus» (Цифровой Иисус).

Хэрригану было всего 22. Он был одним из четырех белошляпых, кто поделился с

Форбс своей историей в прошлом году. Он хитро использовал свои 15 минут славы и выиграл стартовый капитал для бизнеса — профессионального хакерского магазина в финансовом квартале Сан-Франциско.

Идея была проста: корпорации платили его компании Microcosm Computer Resources, чтобы она прогнала их сети через настоящие хакерские атаки и оформила детальный отчет сильных и слабых местах в безопасности. Бизнес «пентестинга» (теста на проникновение) – как это было названо – управлялся большой пятеркой бухгалтерских фирм, но Хэрриган мог поручится перед клиентами в том, в чем не могла ни одна из счетных контор: его опыт исходит из реальной практики взлома и он нанимает других бывших хакеров.

Расценки MCR были от 300$ до 400$ за рабочий час, сказал Хэрриган. Макс будет работать как субподрядчик, получая от 100$ до 150$. И делать две вещи, которые он любит делать больше всего на свете: взламывать и писать отчеты.

Макс нашел свою нишу. Оказалось, что его целеустремленность приспособила его к тестам на проникновение: он имел иммунитет к фрустрации, пробивая часами клиентские сети, двигаясь от одного вектора атаки к другому до тех пор, пока не найдется правильный путь.

С Максом, делающим реальные деньги в MCR, Кими бросила свою работу бариста и нашла себе более достойную работу обучения студентов аутистов. Пара переехала из крохотной студии в Маунтин-Вью в дуплекс в Сан Хосе. В марте они поженились в церкви при университете в Lakewood в Вашингтоне, где жила семья Кими.

Тим Спенсер и многие из «Голодных Программистов» приехали в Вашингтон, чтобы увидеть как их «трудный ребенок» женится. Родители Макса, его сестра, семья Кими, множество друзей и родственников показались на церемонии. Макс носил смокинг и улыбку до ушей, Кими сияла в белом свадебном платье и фате. Окруженные семьей и любимыми друзьями они были идеальной парой начинающей совместную жизнь.

Отец Кими – гордо стоявший военный в униформе и ее мама в традиционном ханбуке стояли снаружи. Макс, окруженный своими родителями, улыбнулся в камеру, в то время как над головой собирались тучи в небе Pacific Northwest.

Прошло почти три года с момента как Макс вышел из тюрьмы. Сейчас он имел всё – преданную жену, обещающую карьеру whitehat-хакера и прекрасный дом. Буквально через несколько недель он выкинет это всё.

Глава 5. «Кибервойна!»

По возвращению домой в Сан-Франциско Макса ждало искушение в виде следующей строки кода:

```
bcopy (fname, anbuf, alen = (char *)*cpp — fname);
```

Это была одна из 9 тысяч строк в исходниках Berkeley Internet Name Domain (BIND) – старая балка в инфраструктуре интернета, такая же важная как любой роутер или оптоволоконный кабель. Разработанный в начале 80х на грант DARPA (Defense Advanced Research Projects Agency — агентство передовых оборонных исследовательских проектов), BIND реализовывал масштабируемую систему доменных имен (Domain Name System — DNS), которая подобно распределенному телефонному справочнику переводит понятные человеку строки типа Yahoo.com в числовые адреса, которыми оперирует сеть. Без BIND или его аналогов, мы бы читали онлайн-новости на 157.166.226.25 вместо CNN.com и заходили бы на 74.125.67.100, чтобы воспользоваться Google-поиском.

BIND был одной из инноваций, что сделали возможным бурный рост интернета. Он заменил незрелый механизм, который не позволял интернету расширяться. Но в 90х BIND был также одной из унаследованных программ, которые создавали крупнейшую проблему безопасности интернета. Его код был продуктом времен честности и простоты, когда сеть была уединенная и было очень мало сетевых угроз. Теперь же хакеры постигли все нюансы и глубины и возвращались с, казалось бы, бесконечным набором дыр в безопасности.

Первосвященство сетевых экспертов названное консорциум интернет ПО (Internet Software Consortium — ISC) само себя назначило стражем интернет-кода и лихорадочно его переписывало. Но в то же время большинство современных сложных сетей в мире со сверкающими новыми серверами и рабочими станциями были запущены с дырявой компьютерной программой из прошлой эпохи.

В 98-м эксперты по безопасности обнаружили последнюю уязвимость в коде. Она сводилось к той одинокой строке кода вначале главы. Она принимала запрос из интернета и, как и положено, копировала его побайтно во временный буфер «unbuf» в память сервера. Но она не корректно проверяла размер входящих данных. Следовательно, хакер мог намеренно передать слишком длинный запрос к BIND-серверу, переполнив буфер и выбросить данные в остальную часть памяти, как

нефть из Эксон Валдез.

Если выполнить такую операцию бессистемно, то это приведет к краху программы. Однако осторожный хакер может сделать нечто более жуткое. Он может загрузить в буфер собственный фрагмент исполняемого кода и затем, избегая падения, подниматься к вершине пространства памяти программы, достигнув зоны кратковременного хранения данных называемого «стэк».

Стэк – то место где процессор хранит информацию о том, что он делает – каждый раз, когда программа перенаправляет компьютер к подпрограмме, процессор «выталкивает» текущий адрес в стэк как закладку, и потому процессор знает куда возвращать данные когда они будут готовы.

После того как хакер оказался в стэке он может перезаписать адрес для возвращения данных на адрес с вредоносным кодом. Когда компьютер закончит с текущей подпрограммой, она вернется не туда где началась, а к инструкциям хакера, и поскольку BIND запускался с привилегиями администратора (root), хакерский код тоже выполнится из под root. Теперь компьютер под контролем хакера.

Две недели спустя после того как Макс и Кими поженились, финансируемая правительством компьютерная группа реагирования на чрезвычайные ситуации университета Карнеги Меллон (CERT - Computer Emergency Response Team), запустившая систему экстренных рассылок о дырах в безопасности, выпустило предупреждение об уязвимости в BIND со ссылкой на простой способ ее исправления: две дополнительные строки кода, что отсеивали слишком длинные запросы. Но исправление CERT содержало также и две других уязвимости, что были следствием исправления и отражали заниженную оценку важности дыры. Таким образом, далеко не все осознавали серьезность ситуации.

Макс осознавал ее прекрасно.

Он прочитал рекомендации CERT с изумлением. BIND шел предустановленным в Linux и запускался на серверах в корпоративных, ISP, некоммерческих, образовательных и военных сетях. Он был везде. Был со столь дефективной строкой кода. Единственное, что сдерживало ожесточенные атаки то, что никто не написал эксплоит (программа эксплуатирующая уязвимость) для этой дыры. Но это был вопрос времени.

Конечно, 18 мая эксплоит появился на Rootshell.com – сайте с новостями о компьютерной безопасности, созданном энтузиастами. Макс снял трубку и позвонил Крису Бисону, своему контакту в ФБР. Ситуация серьезная, пояснил он. Любой, кто не установил патч на BIND мог быть взломан любым скрипт-кидди

способным скачать эксплоит и ввести команду.

Если окунутся в историю, то окажется, что правительственные компьютеры были особенно уязвимы. Всего лишь месяцем ранее, менее серьезный баг в Sun Solaris привел к взлому компьютеров на десятках военных базах США, который заместитель министра обороны назвал «самой организованной и систематической атакой на сегодняшний день» на системы противоракетной обороны. Эти атаки подняли полномасштабную тревогу кибервойны: Пентагон дал им кодовое название «Восход Солнца» и считал главным подозреваемым Саддама Хусейна, пока следователи не вышли на молодого израильского хакера, который просто игрался.

На следующий день Макс снова позвонил Бисону, когда хакерская группа ADM выпустила готовую к использованию версию BIND-эксплоита, который сканировал интернет в поиске непропатченных серверов, вторгался в них, устанавливал себя и использовал зараженный компьютер для последующих сканов и взломов. Определенно, теперь кто-то мог завладеть всем интернетом. Вопрос только «Кто?». Он повесил трубку и задумался. Кто-то собирался это сделать…

В восторженных, мальчишеских тонах Макс поделился своими планами со своей невестой. Макс мог бы стать автором своей собственной атаки на BIND. Его версия могла бы закрыть уязвимость везде, где ее удастся найти, как плодовые мушки заполняют всё своими личинками. Он бы ограничил свою атаку целями наиболее нуждающимся в обновлении безопасности: армия США и правительство.

«Не попадись», сказала Кими. Она научилась не спорить с Максом в состоянии, когда он заложник идеи.

Макс боролся с двойственной природой своей личности: женатый профессионал столкнувшийся с мировой угрозой и импульсивный ребенок любящий пошалить. Ребенок выиграл. Он сел за клавиатуру стал неистово программировать.

Его код работал в три коротких этапа. Начиналось с того, что программа бросала виртуальный крючок, через дыру в BIND, выполняла команду, которая заставляла машину обратиться к интернету и импортировать 230 байтов скрипта. В свою очередь, этот скрипт подключался к уже зараженным хостам, откуда скачивался большой вредоносный пакет, называемый «руткит».

Руткит – это набор стандартных системных программ измененных для того, чтобы служить хакеру: измененная программа входа в системы работает так же как и оригинальная, но теперь она включает в себя, бэкдор, через которую взломщик снова может зайти на машину. Программа «passwd» все также позволяет пользователям менять пароли, но теперь она еще записывает и хранит эти пароли там, откуда их можно потом достать. Новый «list» отображает содержимое

директории как обычно, за исключением сокрытия файлов, которые являются частью руткита.

После того, как руткит был установлен, код Макса мог бы сделать то, что правительство сделать не в состоянии: он бы мог обновить на взломанном компьютере BIND и закрыть дыру в безопасности, через которую он сам и вошел. Компьютер теперь был бы в безопасности, но Макс как доброжелательный вторженец, все еще мог бы повторно зайти в систему если только он этого захочет. Макс исправлял проблему и пользовался ей. Он был и black hat и white hat одновременно.

Сама атака займет буквально пару минут. В первое мгновение компьютер контролируется системными администраторами. В следующее мгновение закидывается крючок, скачивается скрипт, руткит и теперь компьютер принадлежит Максу.

Макс все еще программировал, когда из ФБР ему позвонили, чтобы спросить об отчете по поводу дыры в BIND. Но федералы профукали свой шанс. Сейчас только код Макса говорил с ним. Ему потребовалось немного времени, чтобы взломать пару машин колледжа, для использования в качестве плацдарма, и, затем, 21 мая он зашел в интернет через краденный аккаунт Verio и… запустил код.

Прекрасные результаты были получены сразу же. «Якорь» Макса сообщал об успехе на его компьютер через Verio dial-up, так что он мог наблюдать за распространением атаки. Взломанные машины отчитывались ему всплывающим окном Xterm на его компьютере. База ВВС Брукса теперь собственность Max Vision… Mc-Chord, Tinker, Offutt, Scott, Maxwell, Kirtland, Keesler, Robins… Его код проник на серверы ВВС, компьютеры армии, машину в кабинете секретаря. Каждая машина теперь имела бэкдор, который мог использовать Макс тогда, когда он захочет.

Макс отмечал свои завоевания как контрольные точки в компьютерной игре. Когда его код охватил сетевое пространство ВМФ, он обнаружил столько непропатченных серверов BIND, что спокойный поток всплывающих окон стал бурлящей горной рекой. При попытке справится с ней, компьютер Макса вырубился.

После небольшого тюнинга код был перезапущен. Пять дней Макс был поглощен своей растущей властью над киберпространством. Он игнорировал е-мэйлы ФБР, которое все еще ждало отчета. «Где отчет?» писал агент Бисон. «Позвони»

Он мог сделать все что угодно с такой властью и взломать почти любую сеть какую захочет. Макс обкатывал свой эксплоит на серверах Id Software (Мескит,

штат Техас), компьютерной компании, что разрабатывала третью часть всемирно известного шутера от первого лица Quake. Макс любил такие шутеры. Он мгновенно оказался в сети компании и после небольшого поиска он вышел из нее с трофеем. Он заявил Кими, что он получил исходники Quake III, самой ожидаемой игры года.

Кими была непреклонна: «Можешь вернуть их на место?».

Вскоре Макс осознал, что его атаки привлекли определенное внимание. Верн Паксон, исследователь из Национальной лаборатории имени Лоуренса в Беркли, заметил сканирование сети с помощью системы BRO – Большой Брат. BRO был экспериментальной системой противодействия взломам с одной единственной функцией. Он тихо работал в сети, просеивал трафик в поисках подозрительной активности и в случае обнаружения таковой сообщал администраторам, что происходит что-то не то.

Паксон написал в CERT полный отчет об атаке. Макс перехватил его и изумился. Исследователь не только обнаружил атаку, но и еще составил список серверов атакованных через сеть университета им. Лоуренса – Макс использовал ее как второй стартовый пункт. Он отослал Паксону анонимное сообщение через root-аккаунт лаборатории:

> Верн, прошу прощение за причиненные неудобства, но я в одиночку исправляю ОГРОМНУЮ ДЫРУ В БЕЗОПАСНОСТИ многих из ваших систем. Я признаю, что появились и новые дыры, но они все запаролены и никогда бы не принесли вреда чьему-либо компьютеру.
>
> Если бы я не сделал это, это бы сделал кто-нибудь другой и мог бы напакостить. Например, школьники оставляющие варез, вырубающие IRC BS и втихую стирая файлы через /bin/rm, когда у них плохое настроение. Убожество.
>
> Вы можете не оценить то, что я сделал, но это ради великого блага. Я бросил все хосты из собранного вами списка. Я не касался их, так как я знаю что вы передали список в CERT. CERT следовало бы нанять людей с моим уровнем навыков. Конечно, при достойной оплате я бы никогда не оставлял руткиты или что-то подобное.
>
> Очень умно, не так ли? Хех. Это бомба. Владельцы сотен, даже тысяч систем, и знающие, что их системы пофиксили между делом… Хм, я больше не займусь подобным дерьмом. Теперь у вас есть все мои инструменты. Это выводит меня из себя…

Хм. Во всяком случае я не хочу, чтобы это произошло снова. Я собираюсь оставить все как есть.

«Взломщик»

Так закончилась пятидневная атака Макса на правительство, с количеством взломанных систем больше, чем он мог посчитать. Он был доволен, что он сделал интернет безопаснее, чем прежде: тысячи компьютеров, что до этого были уязвимы для любого хакера, теперь уязвимы только для одного – Max Vision.

Макс сразу же нырнул в новый, более социально-приемлемый проект: он писал Web-приложение, которое позволило бы любому в интернете просканировать свою сеть на наличие уязвимости к атаке на BIND. Он также задумал более качественный вариант осады, чем та которую он только что завершил. Как и прежде, он сканировал правительственные и военные сети. Но вместо взлома уязвимых компьютеров, он автоматически отсылал e-мэйл с предупреждением для администраторов. Не было необходимости прятаться на взломанным dial-up‘ом. Оба сервиса теперь жили на новом сайте WhiteHats.com.

После двух дней и ночей работы, Макс был по колено в его новом проекте легального хакинга, когда Бисон написал снова ему на электронную почту. «Что случилось? Я думал что ты пришлешь мне письмо».

Макс с трудом смог объяснить своему другу из ФБР, что был занят изучением одной из крупнейших компьютерных брешей в истории. То есть, он сделал акцент на своем новом проекте. «Я почти закончил создание общественного сканера уязвимостей и сайта с патчами, но есть еще некоторые момент, которые нужно доделать» — написал Макс в ответ.

«А, и вот еще червь ADM», добавил он — «я не думаю, что он сильно распространится».

Глава 6. «Я скучаю по преступлениям»

Второго июня, после полудня, Макс открыл дверь своего двухэтажного дома в Сан-Хосе. Поприветствовав Криса Бисона он тут же понял, что влип: помимо агента ФБР на пороге стояли ещё трое в костюмах. В том числе угрюмый начальник Бисона – Пит Трэхон, глава отдела расследований компьютерных преступлений.

В течение месяца после BIND-атаки у Макса было немало хлопот. Он запустил сайт whitehats.com, который тут же стал очень популярным в среде безопасников. Помимо сканера на сайте были размещены свежие оповещения CERT, ссылки на патчи для BIND и внушительный объём материала, написанный лично Максом по червю ADM, где тот был исследован до мельчайших деталей. Никто в сообществе и не подозревал, что Max Vision, стоящий за проектом whitehats.com, лично продемонстрировал всю серьёзность уязвимости в BIND.

Макс всё так же продолжал подавать отчёты в ФБР. Получив последний отчёт, Бисон отправил электронное письмо, вероятно, чтобы обсудить свежие достижения Макса: «Что если мы встретимся у тебя? Я знаю адрес, он должен быть у меня где-то записан».

Уже стоя на пороге Бисон раскрыл настоящую причину визита. Он знал всё об атаке Макса на Пентагон. Один из «костюмов» — молодой следователь ВВС из Вашингтона, назвавшийся Эриком Смитом – выяснил, что вторжение в BIND осуществлялось из дома Макса. У Бисона был ордер на обыск.

Макс впустил их, принявшись извиняться. Он объяснил, что только хотел помочь. Беседа проходила мирно. Макс, польщённый вниманием, увлечённо рассказал о процессе вторжения, описывая все хитрости и трюки, а затем с интересом выслушал Смита. Оказалось, что он выследил Макса через всплывающие сообщения, которые тот использовал для уведомлений о захвате системы. Сообщения проходили через диалап Verio и по официальному запросу провайдер выдал номер телефона Макса – это было несложно. Макс убедил себя, что делает нечто действительно полезное для всей сети, поэтому не стал тщательно заметать следы. Агенты поинтересовались, знает ли ещё кто-нибудь о делах Макса – выяснилось, что его босс имел к этому отношение. Макс сказал, что Цифровой Иисус – Мэтт Хэриган – не полностью отказался от хакерских дел и его компания даже собирается заключить контракт с АНБ.

По распоряжению агентов Макс написал признание. «Мною двигало любопытство и интерес, действительно ли это возможно. Я знаю, что это меня не оправдывает и, поверьте мне, я раскаиваюсь в содеянном, но это возможно».

Когда Кими вернулась домой из школы, федералы всё ещё обыскивали дом. Они, словно олени на выпасе, синхронно повернули головы в её сторону, поняли, что это не хищник и молча вернулись к своей работе. Уходя, они забрали всё компьютерное оборудование Макса.

Дверь закрылась, оставив молодоженов в одиночестве в том, что осталось от их дома. На губах Макса едва начало формироваться извинение, но Кими гневно оборвала его: «Я говорила тебе – не попадайся!».

Агенты ФБР в преступлении Макса нашли для себя выгоду. Трэхон и Бисон вернулись в дом Макса и дали своему бывшему союзнику второй шанс. Если Макс рассчитывал на снисхождение, то должен был на них работать. И написанием отчётов было уже не обойтись. Макс настолько решительно стремился загладить вину, спасти свою жизнь и карьеру, что не просил ничего в письменном виде. Он просто поверил, что если он поможет агентам ФБР, те помогут ему.

Две недели спустя Макс получил первое задание. Банда телефонных взломщиков (фрикеров) только что взяла под контроль телефонную систему компании 3Com и использовала её в качестве личной системы телеконференций. Бисон и Трэхон могли бы подключиться к их нелегальному разговору, но они сомневались в своих способностях выдать себя за хакеров. Макс изучил новейшие методы фрикинга и позвонил в систему прямо с оперативного штаба ФБР, в то время как бюро записывало звонок.

Макс обрисовал некоторые свои достижения и упомянул имена хакеров, которых знал. Этого оказалось достаточно, чтобы убедить фрикеров в том, что Макс был одним из них. Они разоткровенничались и сообщили, что являются членами международной банды DarkCYDE, которая состоит примерно из 35 участников, большая часть которых живёт в Британии и Ирландии. DarkCYDE стремился «объединить фрикеров и хакеров со всего мира в одну могущественную цифровую армию», согласно их великому манифесту. По факту же это были просто дети, балующиеся с телефоном, прямо как Макс во времена учёбы в средней школе. После звонка Бисон попросил Макса оставаться с бандой. Макс поболтал ещё с ними в IRC и сдал историю переписки своим надзирателям.

Удовлетворённые работой Макса агенты вызвали его неделю спустя в федеральное здание в Сан-Франциско, чтобы выдать новое задание. На этот раз ему предстояло отправиться в Вегас.

Макс обвёл взглядом карточные столы, устеленные льняными скатертями, в выставочном зале отеля и казино Плаза. Десятки молодых людей в униформе хакеров – в джинсах и футболках – сидели на корточках перед рабочими станциями или стояли чуть в стороне, изредка указывая на что-то на экране. Для человека со стороны это выглядело дико: провести выходные в Городе Грехов, стуча по клавиатуре как робот, вдали от бассейна, игровых автоматов и представлений. Но для хакеров это было специально организованное командное состязание на проникновение в компьютерную систему и захват наспех возведённой сети. Первая команда, которая оставит свой виртуальный маркер в одной из целей, может рассчитывать на приз в 250 долларов, всеобщий почёт и дополнительные очки за взлом других соперников. Новые атаки и хитрости словно струились из хакерских пальцев, секретные эксплойты доставались с виртуальных арсеналов, чтобы впервые выстрелить на публике. На Def Con – крупнейшем в мире хакерском съезде – соревнования на захват флага каждый год были яркими и эмоциональными, не хуже матча Фишера против Спасского. На Кими это не произвело впечатления, а вот Макс был словно в раю. По всему помещению столы были завалены старым компьютерным оборудованием, всевозможной электроникой, инструментами для вскрытия замков, футболками, книгами и копиями 2600 – популярного ежеквартального хакерского журнала.

Макс заметил Элайса Леви – известного «белого» хакера – и указал Кими на него. Леви, он же Aleph One, был модератором рассылки Bugtraq (это как Нью-Йорк Таймс по компьютерной безопасности) и автором экспресс-руководства по переполнению буфера названного «Крошим стек забавы ради и прибыли для», опубликованного в Phrack. Макс не осмеливался подойти к светилу. Что он мог ему сказать?

Макс, разумеется, был не единственным кротом на Def Con. Это мероприятие начиналось в 1992 как скромная встреча, организованная бывшим фрикером, а сегодня Def Con вырос в легендарный слёт, на котором собирается около двух тысяч хакеров, специалистов по компьютерной безопасности и зевак со всего мира. Они собираются здесь, чтобы вживую встретиться с друзьями, с которыми они завели знакомство в сети, проводить и посещать технические доклады, покупать и продавать разные вещи, напиваться, очень сильно напиваться на вечеринках до утра.

Def Con был настолько очевидно привлекательным для правительства событием, что организатор Джефф Мосс придумал игру «засеки федерала». Хакер, который предположительно обнаруживал правительственного агента в толпе, должен был указать на него и громко сообщить об этом. Если аудитория соглашалась, хакер уносил домой желанную футболку с надписью «Я засёк федерала на Def Con». Частенько подозреваемый агент сдавался и добродушно показывал жетон, давая

хакеру лёгкую победу.

Задание Макса было тем ещё испытанием. Трэхон и Бисон хотели, чтобы он вошел в доверие к коллегам-хакерам, попробовал выяснить их настоящие имена и вывел на обмен публичными ключами PGP – это что-то вроде сургучной печати, которой озабоченные безопасностью гики шифруют и подписывают свои электронные сообщения. На сердце у Макса было неспокойно. Написание отчётов для бюро было совсем другим делом, да и угрызений совести по поводу получения данных от фрикеров из DarkCYDE он не испытывал – ребята слишком молоды, чтобы вляпаться в крупные неприятности. Но это задание попахивало доносительством. Личная преданность была записана очень глубоко в прошивку Макса и одного только взгляда на публику Def Con ему хватило, чтобы понять: это его друзья. Многие хакеры прекращали свои незрелые шалости, переходили в легальный бизнес доткомов или основывали собственные компании. Они становились «белыми», как Макс. На конференции это настроение отлично передавала популярная футболка с надписью «я скучаю по преступлениям».

Макс решил проигнорировать задание ФБР и принялся посещать встречи и переговоры. В расписании на этот год значился долгожданный релиз от команды «Культ Мёртвой Коровы». КМК буквально были рок-звёздами в мире хакеров: они записывали и исполняли музыку, а их презентации на съезде были поставлены весьма театрально, что сделало их любимчиками СМИ. В этот раз группа представила Back Orifice – изысканную программу удалённого управления для windows-машин. Если бы вам удалось обманом убедить кого-то запустить Back Orifice, вы бы получили доступ к их файлам, могли бы видеть всё, что происходит на экране и даже посмотреть через их вебкамеру. Программа была разработана, чтобы пристыдить Майкрософт за отвратительную безопасность в Windows98. Все присутствующие на презентации Back Orifice были в восторге, и это настроение передалось Максу. Но ещё больший практический интерес у Макса вызвал доклад о законности компьютерных взломов, который вела Дженнифер Граник – адвокат по уголовной защите из Сан-Франциско. Граник начала презентацию с разбора недавнего дела о преследовании хакера из Bay Area Карлоса Сальгадо-младшего – 36-летнего ремонтника компьютеров, который лучше всех прочих хакеров отражает будущее компьютерных преступлений.

Из своей комнаты в доме своих родителей в Daly City, в нескольких милях к югу от Сан-Франциско, Сальгадо взломал крупную технологическую компанию и украл базу данных, где хранилось восемьдесят тысяч записей о номерах кредитных карт, их владельцах, почтовых индексах и датах истечения срока действия. До номеров кредитных карт хакеры добирались и раньше, но то, что сделал Сальгадо наверняка обеспечит ему место в книгах по истории киберпреступности. Под псевдонимом «Смак» он вошёл в IRC на канал #carding, где выставил весь список на продажу. Это

то же самое, что выставить Боинг-747 на блошином рынке. В то время андеграунд-сцена онлайн-мошенничества с кредитными картами представляла собой болото из детей и мелких хакеров, которые едва ли продвинулись дальше предыдущего поколения мошенников, выуживающих копирку от чеков из мусорных контейнеров позади торгового центра. Их типичные сделки были в одинаковых ценовых категориях, а разговоры друг с другом полны небылиц и идиотизма. Большая часть дискуссии разворачивалась на открытом канале, куда мог зайти кто угодно из органов и всё прочитать. Вся безопасность кардеров основывалась на предположении, что они никому не интересны.

Удивительно, но Сальгадо нашел потенциального покупателя в #carding – студента кафедры компьютерных наук из Сан-Диего, который оплачивал своё обучение, вытаскивая из почтовых ящиков банковские выписки, получая оттуда номера счетов и подделывая кредитные карты. У студента была масса контактов, которые, как он полагал, могли бы купить всю украденную базу у Смака за шестизначную сумму. Сделка пошла немного не так, когда Сальгадо, решивший принять меры предосторожности, взломал Интернет-провайдера покупателя и пошарился в его файлах. Когда студент об этом узнал, он разозлился и тайно начал работать с ФБР. Утром 21 мая 1997 года, Сальгадо прибыл в зал для курения Международного аэропорта Сан-Франциско на встречу со своим покупателем. Предполагалось, что здесь он обменяет компакт-диск с базой на кейс, в котором будут лежать 260 тысяч долларов наличными. Вместо этого он был арестован отрядом по борьбе с компьютерными преступлениями Сан-Франциско.

Сорванная сделка стала откровением для ФБР: Сальгадо стал первым из новой породы жадных до денег хакеров, и он представляет угрозу для будущего электронной коммерции. Результаты опросов показали, что веб-пользователи обеспокоены необходимостью отправки номера кредитных карт в электронном виде – это главная причина, удерживающая их от покупки. Теперь, после многолетних попыток завоевать доверие потребителей и вознаградить веру инвесторов, электронные компании начали покорять Уолл-стрит. Менее чем за две недели до ареста Сальгадо, Amazon.com вышел на IPO и стал за один день на 54 миллиона долларов богаче. IPO Сальгадо было бы выше: общая сумма лимитов по всем кредитным картам в базе составила более миллиарда — $ 931 568 535, если отнять потраченные законными держателями деньги.

Как только Сальгадо арестовали, он во всем признался ФБР. Граник сказала хакерам, что это было его большой ошибкой. Несмотря на сотрудничество, Сальгадо был приговорен к тридцати месяцам тюрьмы в начале этого года.

«Так, ФБР хотели, чтобы я вам сказала, что признание Сальгадо помогло ему», — Граник выдержала паузу, — «Это чушь. Отказывайтесь и молчите!» — сказала она

и с мест послышались одобрительные возгласы, — «Нет никакой пользы от разговора с полицейскими. Если вы собираетесь сотрудничать, то делайте это после консультации с адвокатом и оформления сделки. Нет смысла отдавать им информацию бесплатно».

В задней части комнаты, Кими ткнула Макса под рёбра. Всё, что Граник советовала взломщикам не делать, Макс делал. Всё делал. А сам Макс вновь задумался о своей договоренности с федералами.

• • •

«Мы должны сделать кое-что изменить в схеме нашей работы.»

Макс читал последнее сообщение от Криса Бисона и чувствовал расстройство, которое словно излучалось от экрана. Макс вернулся с Def Con с пустыми руками, а затем не явился на совещание в федеральном здании, где он должен был получить новое задание, чем взбесил начальника Бисона – Пита Трэхона. В следующих строчках письма Бисон предупредил Макса о мрачных последствиях, если тот продолжит юлить.

«В будущем неявка на встречу без уважительной причины будет расценена как отказ от сотрудничества с вашей стороны. Если вы откажетесь от сотрудничества, мы будем ВЫНУЖДЕНЫ принять соответствующие меры. Пит встречается с прокурором по ВАШЕМУ делу в понедельник. Он хочет встретиться с вами в ближайшее время в нашем офисе в 10:00 ровно, В ПОНЕДЕЛЬНИК, 8/17/98. На следующей неделе меня не будет (вот почему я хотел встретиться с вами на этой неделе), так что вы будете иметь дело непосредственно с Питом».

На этот раз Макс явился. Трэхон объяснил, что его заинтересовал босс Макса в MCR, Мэтт Хэриган. Агент был встревожен, что хакер управляет магазином кибербезопасности, где работают другие хакеры, типа Макса, да ещё и пытается претендовать на контракт с АНБ. Если Макс хотел осчастливить ФБР, ему требовалось заставить Хэригана признать, что он по-прежнему занимается взломом и имеет отношение к атаке Макса на BIND.

Агент дал Максу новую форму на подпись. Это было письменное согласие Макса для установки на него прослушивающего устройства. Трэхон вручил ему записывающее устройство, замаскированное под пейджер.

По дороге домой, Макс обдумывал ситуацию. Хэриган был его другом и напарником в хакинге. Нынешнее требование ФБР заставляет Макса пойти на невероятное предательство и стать для Цифрового Иисуса настоящим Иудой.

На следующий день Макс встретился с Хэриганом в закусочной Denny, в Сан-Хосе, без «жучка» ФБР. Он оглядел других посетителей и посмотрел в окно на стоянку. Там в любом месте могли быть федералы. Он вытащил кусок бумажки и протянул его через стойку. «Вот, что происходит…»

После встречи Макс позвонил Дженнифер Граник — он взял её визитку, когда она закончила выступление на Def Con — и она согласилась представлять его интересы.

Узнав, что Макс заручился поддержкой адвоката, Бисон и Трэхон, не теряя времени, официально разжаловали его из информаторов. Граник принялась обзванивать ФБР и офис прокурора, чтобы выяснить планы правительства на её нового клиента. Три месяца спустя она, наконец, получила ответ главного прокурора по киберпреступлениям из Кремниевой Долины. Соединённые Штаты более не заинтересованы в сотрудничестве с Максом. Теперь он мог рассчитывать только на возвращение в тюрьму.

Глава 7. «Max Vision»

Когда сотрудничество с правительством прекратилось, Макс, несмотря на гнёт федерального расследования, принялся нарабатывать себе репутацию «белого» хакера.

Раскрытие уязвимости в BIND и последовавший за этим успех сайта whitehats.com стали хорошим подспорьем для Макса. Теперь он позиционировал себя в качестве консультанта по компьютерной безопасности и создал сайт, где рекламировал свои услуги. Нанять Макса можно было за сто долларов в час, а некоммерческим организациям он помогал бесплатно. Самым весомым его аргументом было стопроцентное проникновение в исследуемую сеть – осечек не было ни разу.

Это было замечательное время для «белых» хакеров: бунтарский дух, который двигал open-source сообщество, проник в сферу информационной безопасности. Выпускники колледжа и отчисленные студенты, бывшие и нынешние «чёрные» хакеры разрушали устои компьютерной безопасности, которые за десятки лет стали привычным делом.

Например, принцип сокрытия уязвимостей в системе безопасности и методов взлома, которые были известны только в узком кругу доверенных лиц, «белые» хакеры называли «безопасность через неясность». Новое поколение предпочитало «полное раскрытие» – так как совместное обсуждение проблем безопасности позволяло не только оперативно их исправлять, но и учиться на ошибках, что было выгодно и хакерам, и безопасникам. Замалчивание уязвимостей было на руку только тем ребятам, которые их использовали в корыстных целях и корпорациям типа Майкрософт, которые предпочитали исправлять свой позорный код по-тихому.

Движение за «полное раскрытие» породило список рассылки Bugtraq, где хакеры любых убеждений могли опубликовать подробный отчёт о найденных уязвимостях. А ещё лучше — предоставить эксплойт: код, демонстрирующий наличие уязвимости. В рамках сообщества более этично было сперва оповестить разработчика и дать ему время на исправление уязвимости, а уже затем публиковать на Bugtraq эксплойт или отчёт. Но сам Bugtraq цензурой не занимался, поэтому случалось, что в список попадал ранее неизвестный баг и за несколько минут о нём узнавали тысячи хакеров и специалистов по безопасности. Такой манёвр гарантировал привлечение внимания разработчика и оперативное исправление ошибки. Таким образом, Bugtraq позволял хакерам демонстрировать свои умения

без нарушения закона. Взломщики же теперь противостояли активно развиваемому сообществу «белых» хакеров и их растущему арсеналу оборонительных инструментов.

Один из лучших таких инструментов разработал в конце 1998го бывший подрядчик отдела кибербезопасности АНБ – Марти Рош. Он решил, что будет интересно узнать о случайных атаках, которые могли бы проскочить через его домашний модем, пока Рош был на работе. В качестве проекта выходного дня он разработал пакетный сниффер под названием Snort и выложил его в сообщество open-source.

Поначалу Snort ничего особенного из себя не представлял – снифферы, которые перехватывали сетевые пакеты и складывали их в дамп-файл для дальнейшего анализа, широко использовались и ранее. Но уже через месяц Рош превратил свою программу в полномасштабную систему обнаружения вторжений (IDS), которая оповещала оператора, едва завидев в сети признаки атаки, уже известной системе. На рынке было представлено несколько таких проприетарных систем, но универсальность и распространение исходных кодов Snort сразу привлекли внимание «белых» хакеров, которые обожают играться с новыми утилитами. Многие энтузиасты тут же примкнули к проекту и стали наращивать функционал программы.

Макс был в восторге от Snort. Эта программа была похожа на БРО – проект лаборатории им. Лоуренса в Беркли, который помог отследить Макса во время его BIND-атаки. Макс понимал, что эта программа способна изменить правила игры в мире интернет-безопасности. Теперь «белые» хакеры могли в реальном времени наблюдать за каждым, кто пытается использовать уязвимость, обсуждённую на Bugtraq и других ресурсах

Snort был системой раннего предупреждения — такой же, как сеть радаров НОРАД для контроля воздушного пространства Америки, но только для компьютерных сетей. Недоставало лишь обстоятельной и актуальной базы сигнатур различных атак, чтобы программа знала что искать.

В течение следующих нескольких месяцев база наполнялась неорганизованно. Каждый пользователь добавлял что-то своё и по крупицам удалось собрать таблицу из примерно двухсот записей. За одну бессонную ночь Макс довёл количество записей до 490, увеличив её объём более чем в два раза. Некоторые записи были уникальными, другие позаимствованы из правил Dragon IDS — популярной, но закрытой системы. Такие правила пишутся на основе сетевой активности каждой атаки, которая позволяет однозначно её идентифицировать.

Например, строка `alert udp any any -> $INTERNAL 31337 (msg:"BackOrifice1-scan"; content:"|ce63 d1d2 16e7 13cf 38a5 a586|";)` позволяет обнаружить «чёрного» хакера, который пытается использовать Back Orifice — культовую программу от КМК, которая поразила всех присутствовавших на слёте Def Con 6.0. Из этой строчки Снорт понимает, что входящее соединение через порт 31337 и попытка передать определённую последовательность из двенадцати байт — признак использования бэкдора.

Макс выложил сигнатуры единым файлом на своём сайте whitehats.com, упомянув в благодарностях множество специалистов по безопасности за их вклад, в том числе Ghost32 — своё собственное альтер-эго. Позднее он расширил этот файл в серьёзную базу данных и призвал других спецов добавлять их собственные правила. Он дал базе этих правил яркое название arachNIDS (паукообразСОВые) — от Продвинутый Архив Указаний, Обнаружений и Образцов для Систем Обнаружения Вторжений.

ArachNIDS мгновенно стал популярным и помог снифферу Роша выйти на новый уровень. Чем активнее «белые» хакеры наполняли базу, тем больше она становилась похожа на базу ФБР с отпечатками пальцев – распознать любую известную виртуальную атаку или её разновидность становилось всё проще.

Макс добился признания, разбирая и описывая принцип действия Интернет-червей так же детально, как он разложил червя ADM. Техно-пресса даже начала разыскивать его, чтобы получить комментарии о недавних атаках. В 1999 Макс влился в перспективный проект, который был нацелен на «чёрных» хакеров. Создал его бывший армейский офицер, который использовал знания военной тактики, чтобы возвести сеть из «подставных» компьютеров (HoneyPot'ов или медовых горшочков), которые предназначались для того, чтобы их взламывали. Проект HoneyNet (лакомая сеть) предполагал скрытую установку сниффера в системе, которая выпускалась в большой Интернет без какой-либо защиты: прямо как сотрудница полиции на каблуках и в миниюбке на углу улицы.

Когда хакер пытался взломать HoneyPot, каждый его шаг тщательно записывался и анализировался экспертами по безопасности. А результаты открыто публиковались в соответствии с идеей «полного раскрытия». Макс работал в роли сыщика-криминалиста, восстанавливая ход преступлений по перехваченным пакетам и действиям хакера. Его «расследования» позволили обнаружить некоторые секретные, ранее неизвестные техники взлома. Но Макс понимал, что его пушистая «белость» не спасёт от федерального обвинения. На досуге они с Кими размышляли об этом. Они могли бы вместе сбежать в Италию или на тихий остров, начать всё заново. Макс нашёл бы покровителя — кого-нибудь с деньгами, кто оценил бы его способности и щедро оплачивал хакерскую деятельность.

Бездеятельное присутствие правительства стало серьёзной проверкой их отношений. Если раньше они не особо планировали собственное будущее, то теперь и загадывать не могли. Их будущее теперь было им неподвластно и эта неизвестность пугала. Наедине они цапались, а на публике косо смотрели друг на друга.

— Я подписал признание, потому что мы только поженились и я не хотел, чтобы у тебя были неприятности, — сказал Макс. Он винил себя за то, что сам стал HoneyPot'ом: женитьба на Кими давала его врагам очень серьёзное преимущество.

Кими перевелась из местного колледжа De Anza в Калифорнийский университет в Беркли, поэтому они перебрались на другую сторону залива, чтобы жить неподалёку от кампуса. Переезд был определённо удачным для Макса: весной 2000 года компания Hiverworld в Беркли предложила ему работать в популярном доткоме, где уже работали другие «Голодные Программисты» — теперь, правда, довольные и сытые.

Компания планировала создать новую антихакерскую систему, которая бы не только обнаруживала попытки взлома, как Snort, но и активно сканировала сеть пользователя на наличие уязвимостей, чтобы не размениваться на отлов атак, которые всё равно не смогут навредить. Сам автор Снорта — Марти Рош — был сотрудником под номером 11. Макс Вижн должен был стать двадцать первым. Должность хоть и слабая, но перспективная. Первый рабочий день Макса был назначен на 21 марта. Американская мечта, около 2000 года.

Утром 21 марта 2000 года в дверь Макса постучались агенты ФБР. Сначала он подумал, что это «деды» из Hiverworld решили разыграть его. Как бы не так!

— Ни за что не отвечай им! — бросил он Кими, схватив телефон. Он нашёл укромное место на случай если агенты будут высматривать его через окна и набрал Граник, чтобы обрисовать ситуацию: обвинительное заключение, похоже, наконец выдали, агенты ФБР хотят упечь его в тюрьму. Что ему теперь делать?

Агенты, впрочем, ушли. В ордере на арест не предусматривалось вторжение в дом Макса, так что он сорвал их план, попросту не отвечая на стук в дверь. Граник со своей стороны уже звонила прокурору, чтобы попытаться организовать явку в офис ФБР в Окленде. Макс связался со своим новым боссом — техническим директором Hiverworld — и сообщил ему, что не сможет выйти на работу в свой первый день. Он так же пообещал в ближайшее время выйти на связь и объясниться.

Вечерние новости Макса шокировали: подозреваемого в компьютерных взломах хакера Макса Батлера обвинили по пятнадцати пунктам, включая перехват конфиденциальной информации, проникновение в компьютерную сеть и владение

украденными паролями.

Макс провёл в тюрьме две ночи, после чего был доставлен к федеральному судье Сан Хосе, для предъявления обвинений. Кими, Тим Спенсер и добрая дюжина Голодных Программистов заполнили зал заседания. Макс был выпущен под залог в сто тысяч долларов: Тим выписал чек на половину суммы, а оставшееся внёс наличными один из «голодных», который сколотил состояние на доткоме.

Информация об аресте всколыхнула сообщество компьютерной безопасности. Hiverworld в одночасье отозвал предложение о работе — ни одной компании по информационной безопасности не стоит нанимать человека, которого прямо сейчас обвиняют в осуществлении взлома. Всех волновала и судьба базы паукообразCOBых, которая оставалась без куратора.

«Это его проект» — написал Рош в списке рассылки. «Таким образом, принудительно менять куратора и отдавать проект в другие руки — недопустимо». Макс ответил в той же рассылке. Он развёрнуто написал и о своей давней любви к компьютерам, и о будущем развитии систем обнаружения вторжений. Макс предположил, что существование whitehats.com и базы паукообразCOBых будет продолжаться любыми средствами: «Мои друзья и семья оказали мне невероятную поддержку. И мне поступают разные предложения о развитии проектов вплоть до таких векторов, которые наверняка не доведут до добра».

Он выставил себя в качестве жертвы и выступил резко против «варварской охоты на хакеров», а Hiverworld обвинил в нелояльности: «Когда завеса спала и пресса начала проявлять интерес, Hiverworld решил прекратить наши отношения. Корпорация струсила, что очень печально. Я не могу выразить всего того разочарования, которое овладело мной, когда я понял, что поддержки со стороны Hiverworld нет и не предвидится. Я — невиновен, пока моя вина не доказана. И я буду благодарен всем в сообществе, кто осознает это».

Шесть месяцев спустя Макс признал себя виновным. Эта новость практически затерялась в сводке из-за шквала федеральных расследований. В этом же месяце Патрик «MostHateD» Грегори, лидер хакерской банды с названием globalHell, был приговорён к двадцати шести месяцам тюрьмы и выплате штрафа за серию дефейсов сайтов на общую сумму чуть больше полутора сотен тысяч баксов. В то же время было предъявлено обвинение двадцатилетнему Джейсону «Shadow Knight» Дикману за взлом систем университета и НАСА, который тот осуществил ради забавы. А шестнадцатилетний Джонатан «C0mrade» Джеймс получил 16 месяцев тюрьмы за то, что в свободное время вламывался в сети Пентагона и НАСА — он стал первым несовершеннолетним, которого посадили за хакерство.

Со всех сторон казалось, что сейчас-то федералы уверенно противостоят компьютерным вторжениям, которые наводили страх на корпорации Америки и госорганы. На самом деле они вели борьбу против «вчерашних» кибервоинов — домашних, «прикроватных» хакеров, чей вид практически вымер. Даже когда Макс стоял в зале суда, ФБР расследовало угрозу двадцать первого века на дистанции в пять тысяч миль, тесно связанную с будущим Max Vision.

Глава 8. «Добро пожаловать в Америку»

Двое русских чувствовали себя как дома в маленьком офисе в Сиэтле. Двадцатилетний Алексей Иванов печатал на клавиатуре компьютера, а его коллега, девятнадцатилетний Василий Горшков, стоял и наблюдал. Сразу после прилета из России они ушли с головой в крупнейшее собеседование их жизни – переговоры о прибыльном международном партнерстве с американским стартапом в области компьютерной безопасности Invita.

Офисные работники мелькали вокруг них и попсовая музыка лилась из компьютерных колонок. Через несколько минут Горшков переместился к компьютеру, в другом конце комнаты и Майкл Паттерсон, генеральный директор Invita, начал разговор.

Паттерсон был тем, кто пригласил русских в Сиэтл. Он сообщил им в письме, что Invita молодая компания, но она набирает клиентов с помощью контактов и связей учредителей, наработанных ими во время работы в Microsoft и Sun. Сейчас компании необходима помощь для расширения в Восточной Европе. Иванов, утверждалось, как и многие талантливые двадцатилетние программисты, работающие с ним, казался идеальным кандидатом для этой работы; Горшков был человеком за компанию, приглашённым Ивановым в качестве пресс-секретаря их дуэта. Дома у него была невеста, беременная его первым ребенком. Паттерсон вскользь начал разговор о недавней цепи атак на компьютеры американских компаний, некоторые из которых платили деньги атакующим, чтобы остановить их. «Просто, если вы ребята так же хороши, как я думаю,» сказал Паттерсон, «мог ли кто-то из вас участвовать в этом?»

Горшков – одетый в тяжелую куртку, которую он носил дома в Челябинске, мрачном, загрязнённым промышленностью городе в Уральских горах, задумался, но все же ответил. «Несколько месяцев назад мы пробовали, но мы решили, что это не очень прибыльное дело.»

Русский скромничал. В течении почти года, малые и средние интернет компании по всему США страдали от грабительских кибератак группы, которая называла себя «Экспертная группа защиты от хакеров» — название которое вероятно, звучит лучше на русском языке. Преступления проходили всегда по одному сценарию: Злоумышленники из России или Украины вторгались в сеть жертвы, похищали

данные кредитных карт или другую ценную информацию, после отправляли письмо или факс в компанию, с требованием платы за молчание о вторжении и за исправление уязвимостей в системах безопасности. Если компания не согласиться платить, «Экспертная группа» грозилась уничтожить системы жертвы.

Банда получила десятки тысяч номеров кредитных кард из сетевого информационного бюро, координационного центра финансовых операций в городе Вернон, штат Коннектикут. Провайдер Speakeasy в Сиэтле был подвержен атаке. Sterling Microsystems в Анахайме, штат Калифорния, был взломан, провайдер в Цинциннати, Корейский банк в Лос-Анджелесе, финансовая компания в Нью-Джерси, электронная платежная компания E-Money в Нью-Йорке, и даже маститый Western Union, который потерял почти шестнадцать тысяч номеров кредитных карт клиентов в результате нападения, после которого началось вымогательство $50,000. Когда музыкальный дистрибьютор Universe отказался выплатить $100,000, тысячи номеров кредитных карт их клиентов были размещены на публичном веб-сайте.

Некоторые компании выплачивали небольшие суммы «Группе экспертов», пока в ФБР делали все возможное для отслеживания вторжений. В конце концов они нашли одного из главарей, им был «subbsta», чье настоящее имя было Алексей Иванов. Это было не так трудно, хакер был убежден, что он вне досягаемости американского правосудия и поделился своим резюме на Speakeasy в ходе вымогательства.

Российская полиция игнорировала дипломатические запросы о задержании и допросе Иванова, поэтому федералы создали Invita, полномасштабный бизнес, как прикрытие для вовлечения хакера в ловушку. Теперь Иванов и Горшков были окружены агентами ФБР под прикрытием, выдававшими себя за сотрудников компании, наряду с «белым» хакером из близлежащего университета Вашингтона, который играл роль компьютерного гика по имени Рэй. Скрытые камеры и микрофоны записывали все в офисе, а установленное ФБР шпионское ПО фиксировало каждое нажатие на клавиатуре. На стоянке снаружи, находилось около двадцати агентов ФБР, готовые помочь с арестом. Агент играющий генерального директора Паттерсона пытался выведать у Горшкова больше. «А что на счет кредитных карт? Номера кредитных карт? Что-нибудь вроде этого?»

«Пока мы здесь, мы никогда не скажем, что у нас был доступ к номерам кредитных карт», ответил хакер.

Агент ФБР и Горшков одновременно засмеялись. «Понятно. Я понял, понял», ответил Паттерсон.

Когда двухчасовое совещание было завершено, Паттерсон отвел парней в

машину, якобы, чтобы отвезти их в арендованное для них жилье. После короткой поездки машина остановилась. Агенты распахнули двери и арестовали россиян.

Вернувшись в офис агент ФБР понял, что установленный на компьютерах компании Invita кейлогер преподнес ему редкую возможность. Следующее что он сделал, могло сделать его первым агентом ФБР, которого российская федеральная полиция обвинила в совершении компьютерного преступления. Он заглянул в журнал кейлогера и извлек из него данные для доступа к компьютеру в Челябинске. Затем, после согласования с руководителем и федеральным прокурором, он удаленно подключился к российскому серверу хакеров и начал скачивать названия директорий и искать файлы, связанные с Ивановым и Горшковым.

Когда он их нашел, он слил 2,3 гигабайта сжатых данных и записал их на диск, и только после, был получен ордер от федерального судьи на поиск в скачанной информации. Это было первым международным изъятием доказательств посредством взлома.

Когда федералы начали копаться в данных, поразительная сфера активности Иванова стала ясна. Помимо вымогательства, Иванов разработал пугающе эффективный способ обналичивания украденных карт, используя специальное программное обеспечение для открытия счетов на PayPal и аккаунтов на eBay и последующего участия в торгах на выставленные товары с помощью одной из полумиллионной коллекции украденных кредитных карт. Когда программа выигрывала аукцион, товар отправлялся в Восточную Европу, где человек Иванова получал его. Потом программа делала это снова и снова. В PayPal проверили список украденных кредитных карт со списком из внутренних баз данных и обнаружили, что ими были поглощены ошеломляющие $800,000 в мошеннических операциях.

Это был первый толчок в тектоническом сдвиге, который коренным образом изменил Интернет на следующее десятилетие. Может быть, навсегда. С первоклассными техническими университетами, но лишь с несколькими легальными направлениями для выпускников, Россия и бывшие советские республики стали инкубаторами для новой породы хакеров.

Некоторые, как Иванов, сделали свои состояния на грабежах пользователей и компаний, будучи защищёнными коррумпированными или ленивыми правоохранительными органами в их родных странах со слаборазвитым международным сотрудничеством. Другие, как Горшков, были вовлечены в преступления из-за трудной экономической ситуации. Хакер окончил Челябинский государственный технический университет по специальности инженер-механик и погрузился в небольшое наследие своего отца, компанию, занимающуюся хостингом и веб-дизайном. Несмотря на самодовольную хакерскую мужественность

в Invita, Горшков был последним дополнением в банде Иванова, он оплатил свой собственный путь в Америку в надежде на улучшение своего финансового положения. В каком-то смысле это у него получилось, после ареста в Сиэтле, он зарабатывал 11 центов работая в тюрьме на кухне или занимались уборкой, и это было больше, чем социальная помощь, которую получала дома его невеста.

После ареста Иванов начал сотрудничать с ФБР, раскрыв список друзей и сообщников, которые продолжали взломы из дома. Бюро осознали, что существуют десятки голодных до денег злоумышленников и мошенников из Восточной Европы уже запустивших свои щупальца в западные компьютеры.

В год это число будет увеличиваться на несколько тысяч. Иванов и Горшков были как Магеллан и Колумб: Их прибытие в Америку мгновенно перекроило глобальную карту киберпреступности для ФБР, бесспорно поместив Восточную Европу в центр этой карты.

Глава 9. «Возможности»

Макс надел спортивную куртку и помятые карго брюки на вынесение приговора и молча наблюдал как юристы начали судебные прения по его делу. Дженнифер Граник, адвокат защиты, сказала судье Джеймсу Вэру что Макс заслуживает смягчения приговора за свою работу в качестве эквалайзера. Прокурор выбрал противоположную точку зрения. Макс, как он утверждал, сделал вид будто он стал информатор ФБР, пока втайне совершал преступления против правительства США. Это было хуже чем если бы он никогда не сотрудничал с ними.

Это был необычный приговор для компьютерного преступника. Дюжина коллег Макса из мира безопасности, посвятившие жизни борьбе с хакерами, написали поручительную на Макса судье Вэру. Драгос Рую, известный евангелист безопасности из Канады, называл Макса «блестящим новатором в этой среде». Французский программист Рено Дерезу признал заблаговременную помощь Макса, которая сделала возможным появление Nessus, сканера уязвимостей Дерезу и одного из самых важных доступных бесплатных средств безопасности.

«Данный Максу потенциал и его ясное видение интернет безопасности… он был бы более полезен обществу в целом, чем оставаясь среди нас как специалист по компьютерной безопасности… вместо того чтобы тратить время в камере и наблюдать как его компьютерный талант переживает медленный, но несомненный упадок».

От технического работника из Новой Зеландии: «Без той работы что сделал Макс… для моей компании и для многих других проектов было бы намного труднее защитить себя от хакеров». От фаната из Кремниевой Долины: «Удаление Макса из нашего сообщества специалистов по безопасности значительно повредило нашу способность защитить себя.» Бывший работник департамента защиты написал: «Заключение этого человека в тюрьму было бы просто издевательством.»

Несколько человек из «Голодных Программистов» также написали письма, как сделали мать Макса и его сестра. В своем письме Кими умоляла об освобождении Макса. «Он сохранил мою жизнь, когда помог уйти от жестокого обращения и научил меня важности самоуважения», - написала она. «Он дал мне убежище, когда мне было негде жить. Он очень хорошо заботился обо мне, когда я была серьёзно больна, сохранил мне жизнь снова отвезя меня в отделение скорой помощи, когда я говорила что «со мной всё в порядке», даже когда я умирала.»

Когда у адвокатов закончились аргументы, Макс говорил за себя, с искренней

учтивостью которую он всегда проявлял вдали от своего компьютера. Свою атаку, он объяснял, благими намерениями. Он только хотел закрыть дыру BIND, но потерял голову. «Я стал слишком заметен», тихо сказал он. «Трудно объяснить чувства того, кто попал в среду компьютерной безопасности… Я чувствовал что в то время я находился в гонке. Что если я зайду внутрь и быстро закрою дыру, я мог сделать это прежде чем люди с худшими намерениями воспользуются ей.

«То что я делал было предосудительно», продолжил Макс. «Пострадала моя репутация среди специалистов по компьютерной безопасности. Пострадали моя семья и друзья.»

Судья Вэр внимательно слушал, но он уже принял решение. Освобождение Макса без тюремного заключения донесло бы неверное послание другим хакерам. «Это нужно для тех кто захочет пойти по твоим шагам, чтобы они знали что результатом является тюрьма», сказал судья.

Приговор: восемнадцать месяцев тюрьмы, сопровождаемые тремя годами во время которых Максу запрещено пользоваться интернетом без разрешения офицера по условному освобождению. Прокурор потребовал от судьи немедленного взятия под стражу Макса, но Вэр отклонил требование и дал хакеру месяц чтобы он привел свои дела в порядок и вернул его маршалам.

• • •

Макс и Кими переехали в Ванкувер, ближе к семье Кими. Когда они вернулись домой, Макс, не теряя времени, организовал Whitehats.com и arachNIDS, чтобы пережить свое заключение. Он установил автоматическую оплату счетов за трафик и выписал список задач для Кими, чтобы она ухаживала за ними в его отсутствие. Теперь она была во главе arachNIDS, сказал он, указывая на сервер расположенный на полу их квартиры. Пара приютила двух котят чтобы обеспечить компанию Кими во время отсутствия Макса и назвала их в честь двух мечей Элрика из Мелнибонэ. Оранжевый котенок был назван Mournblade, серая кошечка была названа Stormbringer.

Макс потратил последний уикэнд на свободе перед своей клавиатурой, готовя передать arachNIDS в управление Кими. Настал понедельник, Макс вовремя закончил свои дела. 25 Июня 2001 года Макс был заключен в окружную тюрьму до его перевозки в новый дом, федеральную тюрьму Тафта, корпоративно-управляемое владение Джорджа Вэкенхута, расположенное рядом с маленьким городком центральной Калифорнии. Макс был обеспокоен этим, поскольку это было ещё одной несправедливостью, подобно возвращению в Айдахо. Он был отправлен обратно в тюрьму не за то что он взламывал, а за то что отказал Мэтту Хэригану. Он

был наказан за свою лояльность, в очередной раз став жертвой своенравной системы правосудия. Он заставил сомневаться судью Вэра, который даже взглянул на детали его дела.

Кими была брошена на произвол судьбы, оставшись в одиночестве в первый раз после того как она встретила Макса. После всех разговоров о том, что они будут всегда вместе, он выбрал направление которое гарантирует их разлуку.

Два месяца спустя, Кими разговаривала с ним по тюремному телефону, когда она услышала хлоп! и едкий запах дыма заполнивший её ноздри. Вспыхнула материнская плата сервера Макса. Макс пытался успокоить её, всё что ей нужно сделать — заменить материнскую плату. Он мог во сне сделать это. Макс описывал ей весь процесс, но Кими осознавала, что не хочет попасть в тюрьму как жена хакера.

В августе она отправилась на фестиваль Burning Man в Неваду, чтобы забыть свои проблемы. Когда она вернулась домой, она по телефону и сообщила плохие новости Максу. Она встретила другого. Это было ещё одним предательством. Макс принял новости с жутким спокойствием, расспросил ей о каждой детали: какие наркотики она употребила когда изменяла ему? Какую позицию они использовали? Он хотел услышать как она просит у него о прощении, он дал бы его в мгновение ока. Но это было не то что она просила. Она хотела развода. «Я не знаю, пожалуй, ты можешь больше не думать о нашем будущем», сказала она.

В поисках аннулирования, Кими села на рейс в Калифорнию и поехала в Тафт, где она нервно сидела в комнате ожиданий, её глаза прыгали по стенам с плакатами изображающими сети тюрем Вэкенхута по всей стране. Когда Макса доставили в комнату для посещений он занял своё место рядом со столиком для пикников из нержавеющей стали и начал своё обращение. Он действительно думал о будущем, говорил он ей, он строил планы на их совместное будущее. «Я разговаривал с некоторыми людьми», говорил он, понизив свой голос до шепота. «Людьми, с которыми, я думаю, мог бы работать».

Джеффри Джеймс Норминтор был в конце своего двадцати семи месячного пребывания, когда Макс встретился с ним в Тафте. В свои тридцать четыре года, Норминтор имел невозмутимый внешний вид дебошира, с толстой шеей, сверхгабаритным лбом и ямочкой Кирка Дугласа на подбородке. Алкоголик и опытный мошенник, он был финансовым волшебником, который делал свою работу лучше, когда был наполовину трезв. Он начинал пить Coors Lights как только вставал с постели, и к концу дня он становился бесполезен, но во время наилучшего восприятия, между утренней трезвостью и полуденной размытостью, Норминтон был мастером игры по крупному, криминальным волшебником, тем кто мог

создавать семизначные суммы из воздуха.

Последняя шалость Нормінтона требовала немного больше чем телефона и факс машины. Целью был Entrust Group, Пенсильванский инвестиционный дом. Летним днем 1997 года Нормінтон взял телефон и позвонил вице-президенту Entrust, представившись инвестиционным менеджером Highland Federal Bank, реального банка в Санта-Монике, Калифорнии. Выделяясь уверенностью и обаянием, мошенник убедил Entrust приобрести депозитные сертификаты банка, обещая вице-президенту вернуть откат в 6.2 процента после одного года инвестирования. Когда Entrust с удовольствие перевели $270,000 в Highland, деньги осели на счету подставной компании сообщника Нормінтона, созданной от имени Entrust. В банке транзакция выглядела как будто инвестиционный дом перевел деньги из одного своего филиала в другой. Мошенники сразу сняли все кроме $10,000 и снова запустили аферу, на этот раз партнер Нормінтона сделал звонок тому же вице-президенту от лица другого банка, City National, предлагая больший откат. Entrust сразу же отправили две транзакции на общею сумму $800,000.

Нормінтона погубила его амбиция. Он отправил сообщника в City National забрать $700,000 одним чеком. Сотруднику банка это показалось подозрительным и он отослал деньги обратно настоящему Entrust. На следующей обналичке уже ждали сотрудники ФБР. Выдающийся финансовый ум теперь томился в ожидании в Тафте.

Нет худа без добра, без заключения он бы не встретил талантливого хакера, который хочет вернуться в систему. Нормінтон ясно понял что он видит реальный потенциал Макса, и теперь они вместе ходили на прогулку каждый день, обмениваясь историями и фантазиями насчет того как они смогут работать вместе, после того как они выйдут на свободу. Под руководством Нормінтона Макс мог быстро научиться взламывать брокерские компании, где-бы они могли действовать с переполненными торговыми счетами и сливать их в офшорные банки. Один большой куш и им хватит денег до конца жизни.

Через пять месяцев Нормінтон и его планы были отправлены домой в солнечный Ориндж, Калифорния, пока Макс отбывал в Тафте ещё год своего срока, утомленный плохим питанием, нахождением под надзором, звуком цепей и ключей.

В августе 2002 Макс был досрочно освобожден и направлен в шестидесяти одноместный реабилитационный центр в Окленде, где он разделял комнату с пятью другими бывшими заключенными. Кими встретилась с Максом чтобы ознакомить его с документами на развод. У неё было всё серьезно с парнем, которого она встретила на фестивале Burning Man; «Настало время», сказала она, чтобы Макс отпустил её. Макс отказался подписать документы.

Относительная свобода Макса в реабилитационном центре была шаткой, учреждение требовало чтобы он получил оплачиваемую работу, иначе он вернется в тюрьму, удаленная работа была запрещена. Он обратился к своим старым знакомым из Кремниевой долины и понял что его потенциал на трудоустройство был подорван широкой оглаской его хакерского осуждение и годом тюрьмы.

Отчаянный, он позаимствовал лэптоп у одного из «Голодных Программистов» и быстро напечатал сообщение, об устройстве на работу, экспертам компьютерной безопасности, которые раньше восхищались им. «Я появлялся в местах, которым тюрьмы передают заключенных в качестве ручной рабочей силы, 5:30 утра, и ещё не нашел работу», написал он. «Моя ситуация просто нелепа.» Он предложил свои услуги по сниженным ценам. «Я готов работать за минимальную оплату следующие несколько месяцев. Конечно если есть открытая вакансия в компании по компьютерной безопасности в этом регионе.… Последние полдюжины работодателей платили мне как минимум $100/час за моё время, сейчас я прошу только о $6.75»

Консультант ответил на просьбу, согласившись дать Максу работу из его домашнего офиса в Фримонте, их разделяла короткая поездка на электричке из реабилитационного центра. Он платил Максу десять долларов в час за помощь в настройке серверов, возвращение к прошлому Макса, на его первую работу вместе с отцом когда он был ещё подростком. Тим Спенсер одолжил Максу велосипед для каждодневных поездок на станцию электрички. Макс освободился из реабилитационного центра через два месяца и «Голодные Программисты» снова активизировались и обеспечили ему убежище. Он переехал в апартаменты в Сан-Франциско, разделяя их с Крисом Тошоком, Сетом Алвесом — ветераном Меридианского состязания отмычек и бывшей девушкой Тошока — Чарити Мэжорс.

Вопреки тюремным фантазиям, он и Нормингтон тайно готовились, Макс был решительно готов идти вперед. Он возобновил свои поиски работы. Но в вакансиях отказывали экс-заключенным. Даже Honeynet Project, куда он пожертвовал свои знания и опыт несколькими годами ранее, остерегались его.

Его дела стали улучшаться в другом направлении: он начал встречаться с сожительницей - Чарити Мэжорс, сбежав из Айдахо, она проектировала себя как олицетворение из виртуального мира, красила ногти как Skittles - разных цветов и носила контактные линзы, которые окрашивают её глаза невероятным изумрудным блеском. Деньги были проблемой для каждого из них: Чарити работала системным администратором порносайта в Неваде, зарабатывая деньги в Серебряном штате, на которые можно было худо-бедно продержаться в Сан-Франциско. Макс был почти на мели.

Один из бывших клиентов Макса из Кремниевой долины пытался помочь Максу заключив с ним договор на $5,000 за выполнение теста на проникновение в сеть компании. Компании нравился Макс и на самом деле их не особо волновало сделает ли он отчет, но хакер взялся за дело серьёзно. Он атаковал фаерволы компании месяцами, ожидая одну из легких побед к которым он привык как white hat. Но он был удивлен. Штат корпорации безопасности улучшился с того времени, когда он работал вместе с ними. Он не мог сделать дыру в сети его единственного клиента. Его 100-процентная успешная репутация рушилась.

«У меня раньше никогда не было неудачных проникновений в систему,» Макс недоуменно сказал Чарити. «Милый, ты не дотрагивался до компьютера годами,» сказала она. «Это займет некоторое время. Не чувствуй себя так, будто ты должен сделать это именно сегодня.»

Макс старался сильнее, но это только сделало его более разочарованным от его бессилия. В заключение он попробовал нечто новое. Вместо поиска уязвимостей на серверах компании, он выбрал индивидуально нескольких работников.

С этими атаками «клиентской стороны» знакомо множество людей, хакерские спам-письма попадающие в их почтовый ящик со ссылкой, которая является электронной открыткой или забавной картинкой. Загрузка исполняемого файла, и если вы игнорируете сообщение об опасности на своем компьютере с Windows и устанавливаете программу, то ваш компьютер не долго будем вашим.

В 2003 неприличный секрет этих атак был в том, что даже опытные пользователи, те кто знают что не нужно устанавливать незнакомые программы могли быть заражены. «Расширения браузера» были в основном этому виной. В девяностых, жуткая война с Netscape за контроль рынка браузеров, сподвигла Microsoft добавить в Internet Explorer лишние свойства и функциональность. Каждая добавленная возможность расширяла возможность атаки на браузер. Больше кода — больше багов. Сейчас дыры Internet Explorer постоянно выходят на поверхность. Они обычно открываются сначала одним из хороших парней: собственными программистами Microsoft или white hat, которые часто, но не всегда, предупреждают компанию, прежде чем детально расскажут о дыре на BugTraq.

Но как только дыру опубликовали, начинается гонка. Black hats работают над применением бага настраивая Веб-страницы использующие атакующий код и тогда пользователи остаются обманутыми после посещения этих страниц. Даже просто просмотр веб-страницы даст контроль над компьютером жертвы без каких-либо признаков заражения. Даже если баги не опубликовали, плохие парни могут понять их с помощью декомпиляции уязвимостей из патчей Microsoft. Эксперты безопасности с ужасом наблюдают, что время между публикацией уязвимости и её

использованием black hats сокращающимся с месяцев до дней. В плохо развивающемся сценарии black hats находят баг первыми: уязвимость «нулевого дня» оставляющая хороших парней в догоняющих.

С новыми патчами Microsoft приходит почти каждую неделю, но даже бдительные корпорации, как правило, отстают в их установке, а обычный пользователь часто не устанавливает их вовсе. Глобальный опрос ста тысяч пользователей Internet Explorer, проведенный примерно в одно время с попытками Макса, определил, что 45 процентов пользователей пострадали от незакрытых уязвимостей удаленного доступа; уменьшение доли американских пользователей лишь немного уменьшило число, к 36 процентам. Атака Макса была эффективной. После получения доступа к компьютеру работника использующего Windows, он перешел в сеть компании изнутри, собрал несколько трофеев и выскочил как разрывающий грудь монстр из Alien.

«Это случилось, тогда я решил избавиться от моей старой модели теста на проникновение и включил клиентоориентированные атаки, как обязательную часть теста», написал он позже white-hat коллеге. «Я был уверен что теперь его репутация составляет 100 процентов»

Но вместо благодарности, последний отчет Макса был принят с возмущением. Использование атаки с клиентского фланга в тесте на проникновение было фактически непристойно; Если вы были бы наняты для проверки физической безопасности в корпоративной штаб-квартире, вы не должны не стеснять ограбить дом работника и украсть ключи. Клиент упрекнул его; они заплатили Максу за атаку на их сервера, а не на работников.

Макс начал задаваться вопросом: есть ли у него будущее в компьютерной безопасности? Его бывшие друзья в сообществе двигались вперед. Hiverworld, где Макс ранее был сотрудником номер 21, сменил свою исполнительную группу и выиграл $11 миллионов венчурного капитала и изменил свое имя на nCircle Network Security. Марти Роеш покинул компанию чтобы привести к успеху Snort - в которую Макс внес свой вклад - фирму, которую он назвал Sourcefire из Мэриленда. Обе компании были на пути к успеху, nCircle начав экспансию которая собрала 160 работников в первые годы и Sourcefire отправились на IPO в NASDAQ. В некоторой альтернативной вселенной, в которой Макс никогда не взламывал Пентагон, или никогда не использовал Verio диалап, или просто хранил свой рот на замке и доносил Мэтту Нэригану, хакер был бы на верху одной из тех компаний имеющих финансовый успех и наградой, интересной работой. Вместо этого он мог только наблюдать со стороны.

Он был скитальцем, цепляющимся за деньги, и волнующийся о том что сделать с

его свободой. Это случилось когда он проверял входящие сообщения на Whitehats.com, он нашел анонимную заметку от «старого друга из Shaft». Это была кодовая фраза Макса, проработанная с Джеффом Нормингтоном. Макс встретил Джеффа в комнате отеля Святого Френсиса, там где они и планировали. Нормингтона не выпустили за хорошее поведение: Его судья, который вынес приговор, требовал ежемесячно предоставлять образцы мочи, чтобы офицер реабилитационного центра был уверен в том, что он не начал пить снова. Что было проблемой, так как он начал пить. После того как он отказался от двух тестов, суд приказал ему провериться на наркотики и алкоголь в реабилитационном центре в Пасадене.

Он вышел через три недели и сейчас, искал аферу после которой хватит нулей чтобы бежать в Мексику. Настало время осуществлять планы сделанные в тюрьме, сказал Нормингтон. Он был готов финансировать Макса в его новой карьере профессионального хакера. Макс был готов. Он достаточно долго старался жить честно, он устал от наказания. Он знал что он износил гостеприимство дома «Голодных Программистов», даже если они не жаловались. Его диета состояла из лапши и овощей. У него не было медицинской страховки и проблем с зубами, стоившими тысячи за их лечение.

Обслуживающий персонал номеров прервал их беседу доставкой приветственной корзины. Нормингтон указал положить корзину в ванную, включил душ, и закрыл дверь - на случай если она содержит жучки. Когда они закончили это смеясь, Макс дал Нормингтону короткий список покупок, вещей необходимых чтобы начать, один высокопроизводительный лэптоп Alienware. И антенну. Большую антенну. Была только небольшая проблема. Нормингтон был на мели. Им нужно было пригласить кого-то ещё для стартового капитала. К счастью Джефф знал такого парня.

Глава 10. «Крис Арагон»

Макс встретил своего будущего друга и напарника по криминалу, Криса Арагона, в маленькой Италии Сан-Франциско — Норт Биче, где обшарпанные стрип-бары и гадалки сосуществовали с приятными, безвкусными пекарнями и летниками с горячей пастой. Встреча была назначена в кафе неподалеку от книжного магазина Сити Лайтс, колыбели поколения битников в 50х годах, по направлению к кафе Везувио, стены которого украшали росписи с винными бутылками и символами мира. Ниже по холму, над финансовым районом, упираясь в небо, стояла Пирамида Трансамерика.

Норминтон представил Криса Максу под приглушенные стуки кофейных чашек и блюдец. Эти двое поладили сразу. Сорокаоднолетний Крис был студентом восточной духовной школы, вегетарианцем, который занимался йогой для концентрации ума. Макс с его замашками хиппи, казалось, нашел родственную душу. Они даже читали общие книги. И, как и Макс, Крис неоднократно имел проблемы с полицией.

Все началось в Колорадо, когда Крису был двадцать один год. Он работал массажистом на курорте, получая достаточно, чтобы платить за аренду жилья и поддерживать кокаиновую зависимость. Однажды он познакомился с буйным ветераном, Альбертом Си, которого он встретил в кабаке, когда тот отбывал наказание. Си был в бегах и ему были нужны деньги, чтобы уехать из страны. Крис был из привилегированной семьи — его мать, Марлен Арагон, работала в Голливуде талантливой певицей. Не так давно она имела радость участвовать в детском утреннем мультфильме Вызов СуперДрузей на ЭйБиСи, озвучивая мстящую кошку Волшебницы Читу. Однако, он также любил романтические образы преступников — в его квартире на стене висел плакат, представляющий собой обложку альбома Вэйлон Дженнингс Леди Любят Беглецов. Крис взял Альберта в дело и предпринял рад смелых, хоть и неудачных, ограблений банков в курортных городах Колорадо.

Первое ограбление в Аспен Сейвингс энд Лоан начиналось неплохо: было утро, когда Крис в бело-синей бандане, прикрывавшей его брекеты, направил армейский автомат 11мм калибра на менеджера банка, чтобы тот открыл сейф. Он и Альберт затолкали менеджера внутрь, где они обнаружили уборщицу, спрятавшуюся под столом, которая вызывала полицию. Горе-преступники в спешке скрылись. Второе ограбление, в окружном банке Питкина, закончилось, не успев начаться. Партнер Криса спрятался в мусорном баке во дворе, планируя выскочить оттуда с оружием,

когда на работу начнут приходить первые сотрудники. План был разрушен, когда Крис, наблюдая с другой стороны улицы, увидел мусоровоз, подъезжающий к баку. Третье ограбление было спланировано лучше. 22 июля 1981 года Крис и Альберт посетили салон Шевроле в Рифле и заявили, что хотели бы попробовать прокатиться на новом Шевроле Камаро. Незадачливый продавец настоял на том, что он поедет с ними, однако, как только они выехали за город, Крис остановился на обочине, а Альберт вышвырнул продавца из машины, угрожая пистолетом. Связав беднягу веревкой, заткнув рот кляпом, грабители бросили его в поле, умчавшись в серебристой спортивной машине.

На следующий день, в 4:50 по полудню, Крис вел украденный Камаро вверх к Вэлли Банк энд Траст в Гленвуд Спрингс, где городские жители тратили свои деньги, которые они зарабатывали в процветающем туристическом бизнесе. Сам Крис был клиентом этого банка. Он ожидал за рулем авто, пока Альберт, в темных очках и с кожаным портфелем, входил в банк. Через несколько минут Альберт выбежал с 10 000 долларов и прыгнул в Камаро, на котором они помчались прочь.

Крис гнал к югу города по грунтовой дороге, которая вилась через скалистые красные холма, вокруг Гленвуд Спринг. Затем они съехали на тропинку, где его подружка ждала с другой машиной. Торжествуя и радуясь, Крис остановился с заносом и поднял столб пыли. Он прыгал и кричал: «Мы сделали это!», когда полицейская машина, едущая на облако пыли, нашла грабителей. Крис и Альберт рванули вверх по скалистым и заросшим горам. Когда Крис споткнулся и упал на кактус, двое полицейских догнали и поймали его. Крис бросил ружье и сдался. Из этой истории Крис вынес урок: самым глупым в этом ограблении было оружие и угнанный автомобиль. Когда, в 1986 году, Крис досрочно вышел после пяти лет в федеральной тюрьме, он увлекся махинациями с кредитными картами и даже имел небольшие успехи. После этого он познакомился с барыгой из Мексики, которого он встретил в кабаке. Крис помог ему с доставкой двух тысяч фунтов (907 кг) марихуаны в двадцатиакровое ранчо, недалеко от Риверсайд, Калифорния, однако сразу же был арестован во время тайной операции отдела по борьбе с наркотиками. В сентябре 1991 года Крис снова попал в тюрьму.

Когда Крис вышел в 1996 году, ему было тридцать пять лет — часть детства и больше половины сознательной жизни он оставил за решеткой. Он пообещал себе не нарушать закон впредь. С помощью мамы он основал бизнес под названием Мишн Пацифик Кэпитал, занимающийся лизингом компьютерной и бизнес-техники для стартап компаний, которые старались быть на волне дот-ком гонки.

Аккуратно подстриженный, приятный, с чарующим взглядом, Крис легко вписался в роль бизнесмена Южной Калифорнии. После жизни полной проблем и неопределенностей, прелести обычной жизни, доступной среднему классу, казались

экзотикой. Он любил ездить по конференциям, встречаться с сотрудниками, нанимать новых людей, болтать с коллегами. На одной из маркетинговых конференций Крис встретил Клару Шао Йен, стильную женщину с китайскими корнями, которая эмигрировала из Бразилии. Очарованный красотой и умом Клары, вскоре он женился на ней. Под руководством Криса Мишн Пацифик заработала репутацию инновационной компании, одной из первых предложив мгновенные контракты через интернет, которые помогали фирме получать десятки тысяч клиентов по всей стране. Грабитель банков и торговец наркотиками в прошлом, Крис имел двух видных бизнесменов Орандж Каунти в партнерах и двадцать одного сотрудника, которые работали в просторном офисе, недалеко от Пацифик Коаст Хайвэй. Клара периодически «светилась» в рекламных журналах и на сайте компании, чтобы помогать компании с продвижением. К 2000-м годам, пара отметилась на всех фронтах — купили роскошный дом в Ньюпорт Бич, родили сына и сделали ставку на улучшение бизнеса до огромных масштабов.

Этой весной мечта умерла. Пузырь интернет-компаний лопнул и поток новых компаний, который был основой Мишн Пацифик, стал иссякать. А после, крупные компании, как Американ Экспресс, вошли в сферу лизинга, вытесняя малые фирмы. Компания Криса была одной из десятков лизинговых контор, которым было суждено рухнуть и прогореть. Он начал сокращать сотрудников, но этого было мало, и ему пришлось признаться оставшимся, что компания больше не сможет оплатить их работу. Крис ушел работать в другую лизинговую компанию, где вскоре он был сокращен, когда прокатилась волна увольнений в связи с продажей фирмы крупному банку. Тем временем его жена родила второго мальчика. Поэтому, когда Джефф Норминтон появился, чтобы обсудить суперхакера, которого он встретил в Тафте, Крис был готов к встрече.

К тому моменту, когда он и Макс встретились в ресторане Норт Бич, Крис уже спонсировал схему Норминтона, обеспечивая того специфическим оборудованием, которое, как сказал Норминтон, было нужно хакеру. Теперь, когда Крис встретил Макса вживую, ему не терпелось увидеть его в работе. После нескольких часов разговоров, трое мужчин вышли из кафе, чтобы найти место, откуда можно было провести взлом. Они поднялись на двадцать седьмой этаж Холидэй Инн в Чайнатауне, в нескольких кварталах от отеля. Они спросили Макса выбрать какую-нибудь комнату повыше дороги. Макс нацелился на окно, включил ноутбук, подключил антенну и начал сканировать Wi-Fi сети.

В 2003 году мир только начинал большое путешествие в беспроводной мир, неся с собой большую дыру в защите. Революция началась с беспроводной точки доступа AirPort от Apple, позже к ней присоединились производители железа Linksys и Netgear. По мере падения цен на железо, все больше и больше компаний и обычных пользователей избавлялись от паутины голубых Ethernet кабелей. Тем не менее,

создание и объединение компаний по всей стране в беспроводную сеть было мечтой хакеров. В большинстве случаев, эти сети использовали беспроводной стандарт 802.11b, включавший в себя схему шифрования, которая, теоретически, была защищена от взлома, прослушки и подключения к чужой сети. В 2011 году, исследователи из Университета Калифорнии в Беркли осветили ряд серьезных недостатков этой схемы, которые позволяли взломать ее доступным оборудованием и нужным софтом. С практической точки зрения, не нужно было прибегать к какой-либо технической черной магии. Чтобы ускорить переход на новое оборудование, производители точек доступа отключали шифрование по умолчанию. Компании просто использовали оборудование с завода, не ковыряясь в настройках, наивно предполагая, что стены офиса спасут их сеть от взлома с улицы.

За несколько месяцев до того, как Макс попал в тюрьму, whitehat-хакер придумал вид спорта, названный вардрайвингом, чтобы показать масштабы дырявых сетей Сан Франциско. После установки антенны на крыше своего Сатурна, whitehat-хакер катался по улицам города, пока его ноутбук сканировал точки доступа Wi-Fi. После часа в финансовом районе города, его установка нашла около восьмидесяти сетей. С тех пор прошло полтора года, и Сан Франциско, как и любой другой большой город, погряз в невидимой сети интернет трафика, доступной любому, кто захотел нырнуть в нее.

Взлом из дома — для идиотов и подростков, — Макс узнал это на своей шкуре. Благодаря Wi-Fi, теперь он мог работать практически из любого места, оставаясь при этом анонимным. В этот раз, если полиция попадет на след Макса, то всё, что они получат — одного из бедных провайдеров, что использовал Макс для подключения.

Антенна, которую использовал Макс была огромной — параболическая сетка из проволоки шириной в два фута, которая мгновенно отслеживала десятки сетей из эфира, окружающего Холидэй Инн. Он выбрал одну из сетей и показал Крису, как это работает. Используя сканер уязвимостей, — тот же софт, что он использовал в тестах на проникновение, — он мог сканировать большие фрагменты интернет адресов в поисках известных уязвимостей, как будто закинув сеть в море интернета. Дыры в безопасности были повсюду. Для Макса не было проблемой проникнуть в сети финансового института или торговой корпорации. Дело было в Нормингтоне и Крисе, чтобы решить, какие данные им были нужны и как они хотели использовать их. Крис вымотался. Этот хакер шести с половиной футов ростом, полу-вегетарианец, знал свое дело, даже если был гнилой до костей.

Крис представил Макса одному из своих тюремных знакомых, мошеннику по недвижимости Вернеру Джанеру, которого Крис встретил в Терминал Айлэнд в 92ом году. Джанер предложил Максу 5000 долларов, если он взломает компьютер

личного врага. Он выписал чек на Чарити, поэтому Максу не пришлось объяснять этот доход своему курирующему офицеру. Полученые деньги дали Максу небольшую передышку. Он начал летать в Орандж Каунти, делая ошибку в имени на билете, чтобы у офицеров не было данных о том, что Крис нарушил границы Бэй Эрия, дозволенные ему нахождением под надзором. Макс и Нормингтон проводили взлом в течение недели, засев в гараже Криса.

Он скачал список небольших финансовых компаний с сайта Федеральной Корпорации Страхования Вкладов, предполагая, что они были наиболее уязвимы для атак, и запустил скрипт для сканирования каждого банка на наличие известных дыр в безопасности. Электронный звонок прозвенел на весь гараж, оповещая о завершении сканирования. Червь прошерстил все банки и вытащил имена клиентов, финансовые данные и проверочные номера чеков. Обобщенный подход означал, что Макса снова ждет разочарование, как это было при последнем легальном тесте на проникновение. Взлом одной единственной цели может быть сложен, в зависимости от цели, это может быть даже невозможно. Но сканирование сотен и тысяч систем дает гарантию, что можно найти что-то слабое. Это было игрой чисел, как пытаться открыть случайно оставленную открытой дверь машины на огромной стоянке.

Только Чарити имела полное представление о том, чем занимается Макс, и ей это не нравилось. Пытаясь добиться ее расположения, Крис и Нормингтон пригласили молодую пару в Орандж Каунти на выходные, собираясь отправиться в Диснейлэнд. Чарити видела, что Макс и Крис ладят, но что-то не давало ей покоя. Он был слишком скользким и слащавым. Макс переключился на небольшие сайты интернет-торговли, где он собирал историю транзакций, в которых иногда попадались номера кредитных карт. Однако этот взлом не был направленным, ни Крис, ни Нормингтон не знали точно, что они будут делать с добытыми данными. К счастью, у Криса были деньги. Вернер Джанер задолжал ему 50 000 долларов и был готов перевести деньги на любой, удобный Крису, счет. Ожидая получить на руки законные, холодные, осязаемые наличные, Крис спросил Нормингтона, как бы поступил он, на что Нормингтон поддержал мнение о том, что лучше сделать перевод на кого-то из друзей, а затем, в течение нескольких дней, уже обналичить его.

Первая часть перевода прошла как и ожидалось, и Нормингтон, и его друг пришли с Крисом и получили 30 000 долларов в 100 долларовых купюрах. Следующий день, однако, не заладился, — Нормингтон сообщил, что его друг заболел и ему нужно отлежаться денек. По правде говоря, Нормингтон узнал источник денег — это был кусок Криса в деле Джанера, где он помог в махинациях с недвижимостью. Это были грязные деньги, и теперь Нормингтон был в этой схеме. На следующее утро Крис нашел Хонду, которую он одолжил Нормингтону, припаркованную недалеко от своего офиса, — одно колесо было пробито, а на крыле виднелась свежая вмятина.

В салоне была записка от Нормингтона: «ФБР гонится за мной. Я сваливаю из города». Крис позвонил другу Нормингтона, догадываясь, что ему скажут: «Самочувствие в порядке, а оставшиеся 20 000 долларов мы уже сняли. Я отдал их Нормингтону. Разве ты не получил их?» Крис разыскал Макса через Чарити и обрушил на него шквал вопросов: что Максу известно о местонахождении Нормингтона? Где его деньги? Макс был удивлен не меньше Криса исчезновением Нормингтона. Обсудив детали, дальше они решили действовать без Нормингтона.

Макс и Крис погрязли в рутине. Раз в месяц Крис прилетал или приезжал на север и встречался с Максом в Сан Франциско, где они заседали в отеле. Они приносили громадную антенну Макса по ступеням в их комнату и устанавливали на треноге, направляя в окно. Затем Макс проводил настройку, отыскивая точку доступа с сильным приемом и высокой скоростью. Они заметили, что при взломе Wi-Fi высота была не столько важна, сколько обзор из окна,. Если у них что-то не получалось, Крис всегда мог попросить другую комнату, объясняя это тем, что он не может поймать сигнал сотовой сети или боязнью высоты.

Для Макса это было работой, прощаясь с Чарити, он исчезал на неделю в одном из лучших отелей города, в Хилтоне, в Вестине, W, или Хайятте. Под лязг трамваев, которые ездили по улицам, Макс сканировал сети, выхватывая любую информацию, что ему попадалась, не представляя, что именно с ней делать. Ему пришло в голову взломать компьютер Кими и ее парня, с которым она уехала. Макс задумывал взломать ее адресную книгу, чтобы разослать письмо от ее имени, в котором он расскажет, как она его предала. Он думал, все должны знать, что новая жизнь Кими основана на предательстве.

Он не сделал этого. У него была Чарити. Кими переехала, так что ничего не изменить, если пытаться пристыдить ее. Вскоре после этого Крис подписал бумаги о разводе. Вернувшись к работе, он начал поиски в Гугле, чтобы определиться с дальнейшими действиями по взлому — «Что делают другие мошенники?», «Как можно использовать украденные данные?» Он был удивлен, когда нашел ответы на свои вопросы на двух сайтах: CarderPlanet и ShadowCrew.

Глава 11. «Дампы по 20$ от Скрипта»

Весной 2001 года около ста пятидесяти русскоязычных компьютерных преступников собрались в ресторане портового города Одессы, чтобы обсудить запуск революционного сайта. Среди присутствовавших был Роман Вега, 37 летний мужчина, который продавал поддельные кредитки через его онлайн магазин БоА Фактори (Bank Of America), киберпреступник, известный как Король Артур и мужчина, который мог бы стать их лидером, украинский продавец кредиток, известный как Скрипт.

Заседание было вызвано успехом Британского сайта Библиотека фальшивок, запущенного в 2000 году. Этот сайт решал одну из основных проблем общения в криминальном бизнесе через IRC чат-румы, где свобода и многолетний опыт преступлений лопнули, как пузырь, стоило чату исчезнуть. Основанная горсткой западных киберпреступников Библиотека фальшивок собрала нелегальные учебники, а также форум, где воришки, занимающиеся махинациями с документами, могли обменяться советами, подсказками, купить и продать «обновки» идентификационных карт — эвфемизм, выдержанный в том же духе, что и «мероприятия» у проституток.

Библиотека фальшивок имела гораздо больше общего с BBS в преддверии появления интернета, чем с IRC. Пользователи могли публиковать сообщения прямо в ветках форума, имели рейтинг и ники. Как только преступники со всего мира обнаружили этот островок в мутном, выдуманном море подпольной торговли, сайт собрал сотни, а потом и тысячи пользователей со всей Европы и Северной Америки. Среди них были люди, совершающие махинации с паспортами, хакеры, фишеры, спаммеры, фальшивомонетчики, кардеры, все, кто прятался в своих квартирах и подпольях, слепые до сего момента, когда открыли для себя обширность этого тайного общества.

Кардеры Западной Европы с завистью наблюдали за Библиотекой фальшивок. Они хотели провернуть этот трюк и в своем подполье. Итогом июньского заседания в Одессе стало появление Международного Союза Кардеров, сокращенно Carderplanet.com. Крепко организованная, переосмысленная Библиотека фальшивок, ставшей пастбищем для подполья бывшей советской империи. В то время как Библиотека фальшивок была беспечным форумом, а БоА Фактори простым, незамысловатым магазином, фanet была дисциплинированным онлайн-рынком по

примеру торговой биржи.

Не стесняясь своих намерений, сайт взял на вооружение пример Итальянской мафии для ведения жесткой иерархии. Зарегистрированный пользователь назывался «sgarrista» — солдат без особых привилегий. Чуть выше располагался “giovane d’honore», человек, который помогал регулировать споры под надзором «capo». На вершине пищевой цепочки был Дон Carderplanet, Скрипт.

Русскоязычные торговцы стекались на новый сайт, чтобы предложить различный спектр товаров и услуг. Номера кредиток были основным товаром, но лишь сначала. У некоторых продавцов, специализирующихся на «полной инфе», можно было раздобыть номер кредитки, имя владельца, адрес, номер страховки и девичью фамилию матери всего за 30 долларов. Взломанные аккаунты eBay стоили всего 20 долларов. Некоторые амбициозные покупатели могли потратить 100 долларов для «изменения счета» украденной карточки — процедуры, когда платежный адрес владельца мог быть изменен на почтовый адрес покупателя. Другие торговцы продавали поддельные чеки, денежные переводы или адреса арендованных квартир в США, где приобретенный товар можно было перепродать мошеннику без страха быть пойманным. В продаже также имелись заготовки кредитных карт с магнитной полосой, «обновки» документов с голограммами, которые, в зависимости от качества, продавались от 75 до 150 долларов. Можно было приобрести набор из десяти документов с одной и той же фотографией, но с разными именами за 500 долларов.

Регистрация на Carderplanet была открыта для всех, но чтобы продавать, торговцы должны были предоставить свои товары или услуги на проверку рецензента. От новых торговцев иногда требовалось разрешение от Скрипта или залог в фонд чрезвычайных ситуаций, который использовался для выплат покупателям, если продавец не выполнил своих обязательств после оплаты. Продавцы были обязаны держать в курсе своих планов на отдых, хранить в безопасности информацию о покупателях и оперативно реагировать на жалобы клиентов. Рипперы, продавцы, которые не могли продать свой товар, банились, как было с любым продавцом, который имел 5 жалоб от клиентов.

Вскоре, подражая Carderplanet, был создан второй сайт, нацеленный на Англоязычные страны, Shadowcrew. В сентябре 2002 года, после ошеломляющего успеха строго организованной Carderplanet, кардер под ником Kidd бросил все силы Библиотеки фальшивок, чтобы развернуть бизнес в России. Новости о сайте распространились в IRC чат-румах, как в тюремных дворах, и к апрелю 2003 года Shadowcrew имел тысячи зарегистрированных пользователей.

С девизом «Для тех, кто любит оставаться в тени» Shadowcrew был и колледжом

на дому, и онлайн супермаркетом всего незаконного.

Их учебники содержали информацию о том, как использовать краденные номера кредиток, подделывать водительские права, взломать сигнализацию, или сделать глушитель для оружия. Сайт мог похвастаться вики, где можно было отследить процесс изготовления водительских прав. Утвержденные торговцы со всего мира предоставляли ошеломляющий спектр незаконных товаров и услуг: кредитные выписки, взломанные банковские аккаунты, имена, даты рождения и номера страховок потенциальных жертв махинаций. Как и на Carderplanet, каждый продукт имел своего специалиста, так что каждый продавец должен был быть проверен доверенным пользователем сайта для того, чтобы он мог продавать что-либо. Споры рассматривались тщательно и рассудительно, — администраторы и модераторы работали сверхурочно, чтобы разоблачить и забанить рипперов, которые продавали пустышки.

Торговля обхватывала не только информационные товары. Спросом пользовались также вещи вроде банкоматных скиммеров, лекарств, которые продавались только по рецепту, кокаин, а также сервисы, предоставляющие услуги по ДДОС-атакам: «уронить» сайт и защитить атаку от обнаружения антивирусами можно было за 200 долларов. Один из проверенных продавцов предлагал сервис для получения технических сертификатов в течение пары дней. Продавец, называющий себя UBuyWeRush «выстрелил», заполняя подполье программаторами магнитных полосок кредиток, а также бумагой с водяными знаками и картриджами с магнитными чернилами для подделки чеков.

Детское порно было запрещено, а один из продавцов, который попросил, чтобы ему разрешили торговать экзотическими животными, был осмеян всем форумом. Но все остальное было разрешено на Shadowcrew.

Тем временем Carderplanet запустил ветку на форуме для преступников из Азии, Европы и Штатов, но уже был ShadowCrew, который основал настоящий международный рынок: смесь Чикагской торговой биржи и баром на Mos Eisley в Звездных войнах, где преступники разных специализаций могли встретиться и обсудить их планы. Мошенник, подделывающий документы, мог купить в Денвере номера кредитных карт у хакера из Москвы, далее отправить их в Шанхай, где из них сделают фальшивые кредитки, а затем забрать фальшивые водительские права у мошенника из Украины прежде, чем отправиться в магазин.

Макс поделился своим открытием с Крисом, который был очарован новыми вещами. Крис зарегистрировался на форумах, стал изучать их содержимое, как учебник. Немногое изменилось с тех пор, как Крис занимался мошенничеством с кредитками в восьмидесятых. Однако, некоторые вещи все же изменились.

Было время, когда жулики могли получать номера кредитных карт буквально из мусорки, после копания в мусорных баках или из следов на барабанах печатающих машин. Теперь же механическая печать практически не используют, Visa и MasterCard настаивают, чтобы чеки по операциям не содержали полные номера карточного счета. Даже если тебе удастся получить полный номер, этого не достаточно, чтобы изготовить фальшивую кредитную карту. Изготовители кредитных карт добавляют специальный уникальный код к каждой магнитной полосе, наподобие PIN кода, неизвестный даже держателю карты. Данный код называется Кодом Проверки Подлинности (CVV) карты. Он генерируется из других данных на магнитной полосе — номера аккаунта и срока годности карточки, — затем шифруется секретным ключом, который известен только банку-эмитенту (выпускающему карточки). При использовании карточки в терминале, CVV код отправляется вместе с данными ksарточки для проверки банком. Если данные не совпадают, то транзакция отклоняется.

После того, как Visa ввела CVV код в 1992 году, доход мошенников стал резко падать — от 0,18% за год со всех операций Visa, до 0,15% год спустя. В 2000х годах инновации доказали, что они способны противостоять фишинг-атакам, при которых спаммеры рассылают тысячи фальшивых писем с целью получить данные кредитных карточек пользователей. Без CVV кода на магнитной полосе, который клиенты не знают, а значит и не могут оставить где-либо, украденные номера кредитных карт становятся бесполезными при операциях. Никто не может отправиться в казино Вегаса и купить черных фишек карточкой, которую получил в ходе фишинговой атаки. MasterCard последовали примеру Visa и выпустили свой собственный Секретный Код Карты (CSC). Далее, в 1998 году, Visa представила CVV2 код — секретный код, который печатается на обратной стороне карты для клиента, исключительно для покупок по телефону или интернету. В дальнейшем это уменьшило потери преступников и воздвигло Китайскую стену между мошенничеством в интернете и в реальной жизни. Данные, украденные из баз сайтов или посредством фишинг-атаки могли быть использованы только при онлайн операциях, в то время как данные магнитной полосы могут использоваться везде, кроме онлайн операций, потому что в них нет CVV2 кода.

К 2002 году меры безопасности превратили данные магнитных полос в один из самых ценных товаров подполья, подставив клиентов под удар. Хакеры начали нарушать работу систем обработки данных карточных центров, но самым обыденным методом получения данных карточек было трудоустройство в фаст-фуд ресторан сотрудника с карманным скиммером, который содержал считыватель магнитной полосы и встроенную память. Меньше, чем зажигалка, скиммер легко помещался в карман фартука работника или костюма метрдотеля, в нем могли храниться данные сотен карточек клиентов, которые в дальнейшем можно было

скачать на компьютер. Мошеннику достаточно секунды, чтобы считать данные с карточки посредством скиммера.

В конце 90х годов мошенники начали веерные наезды в крупные города Соединенных Штатов, в поисках официанток, официантов и прочего обслуживающего персонала, заинтересованных в дополнительном доходе, около 10 долларов за один прогон карточки. Хоть это и было рискованно, некоторые менеджеры АЗС и рабочие могли использовать в работе на примере установки крошечных плат на монетоприемники насосов и терминалов в розничных магазинах. Некоторые данные могли быть использованы на месте, но большая часть «уплыла» в Восточную Европу, где данные продавались десятками, сотнями и даже тысячами за раз. Кардеры называли эти данные дампами, каждый содержал только две строки текста, каждая на своей дорожке, 3 дюйма магнитной ленты.

```
Track 1: B4267841463924615^SMITH/
JEFFREY^04101012735200521000000
Track 2: 4267841463924615=041010127352521
```

Дамп обычной кредитки стоил около 20 долларов, 50 долларов за голд карточку и от 80 до 100 долларов за ограниченную корпоративную карту.

Крис решил попробовать себя в кардинге. Он узнал, что Скрипт, крестный отец CarderPlanet, был самым надежным источником дампов в мире.

Он заплатил украинцу 800 долларов за набор из номеров 20 карт Visa Classic и еще около 500 долларов за MSR206 — любимый ридер карточек с магнитными полосами. После подключения ридера к компьютеру и установки нужного программного обеспечения он мог взять любую подарочную карту Visa или одну из его собственных и расшифровать ее в два быстрых прогона, с одним из дампов Скрипта.

С перепрограммированными картами, прожигающими дыру в его кармане, Крис просматривал свой личный справочник и некоторые розничные магазины, прикидывая возможности. Простое мошенничество с картой несложное и дешевое дело, но оно имело некоторые ограничения. Наблюдая, Крис быстро определил, что покупка электроники и дорогой одежды — дело непростое.

В дорогих магазинах существуют некоторые меры предосторожности — последние четыре цифры номера карты вводит сотрудник; когда цифры не совпадают с кодом магнитной полосы, некоторые POS терминалы отказывают в операции, или хуже того. Перепрограммированные карточки были полезны только там, где ты сам управляешься со своей карточкой — на автозаправках или в

аптеках.

Крис попробовал себя в местном супермаркете. Он без разбора заполнен свою корзину и оплатил товары, проведя карточкой через POS терминал. Через секунду слово «Оплачено» промелькнуло на дисплее и где-то в Америке случайный человек получил счет на 400 долларов за покупку продуктов. Крис отвез свои нечестно приобретенные продукты семейной паре в округе Orange County, которая была в худшем финансовом положении, чем Крис — у мужа украли его рабочие инструменты, поэтому Крис отвел его в магазин, чтобы купить новые. Стали ходить слухи, что у Криса были кредитные карты, которые он стал раздавать некоторым друзьям. Они всегда были достаточно умны, чтобы делать небольшие покупки Крису в качестве благодарности. Крис начинал видеть очертания его бизнес-плана в его операциях с пластиком. «Брось всё остальное, Макс, — говорил Крис. Реальные деньги в дампах».

Глава 12. «Бесплатные Amex!»

За ужином Макс слегка коснулся своего плана с Черити. «Какие бы ты назвала учреждения, которые больше всех заслуживают того, чтобы быть наказанными?» — спросил он.

У него уже был готовый ответ: заёмные компании. Жадные банки и кредитные компании, которые обвели клиентов вокруг пальца на ежегодный долг в 400 миллиардов долларов, подогревая кредитный интерес и подсаживая детей на пластик, прежде чем те закончат колледж. Дело в том, что потребители никогда не несут ответственность за мошеннические сборы – по закону им может быть выставлен счет за первые 50 долларов, но большинство банков отказалось даже от этого — мошенничество с кредитными картами стало преступлением без жертв, оплачиваемое бездушными деньгами этих учреждений.

Кредит не был настоящим, Макс рассуждал о нём как об абстрактном концепте: он крал бы цифры из системы, а не доллары из чьего-либо кармана. Финансовые институты перестали бы держать потребительскую корзину, ведь они заслужили это.

Черити научилась принимать горечь Макса, которая появилась у него после возвращения из тюрьмы. Жить с ним значило никогда не смотреть криминальные фильмы по телевизору, потому что любое изображение полиции как хороших парней распыляло Макса. Она не было полностью уверена, что Макс имел в виду сейчас, и она не хотела этого знать. Но одно было ясно. Макс решил, что он будет Робин Гудом.

• • •

Макс знал, где именно получить данные кредиток, которые хотел Крис. Были тысячи потенциальных источников, которые были на виду как CarderPlanet и Shadowcrew. Сами кардеры были его добычей. Большинство из них не были хакерами, они были просто мошенниками, которые знали немного о мошенничестве и ничего о компьютерной безопасности. Это, конечно, не могло быть труднее, чем взлом Пентагона. Также это было морально приемлемым предложением: он будет красть номера кредитных карт, которые уже были украдены. Преступник собирался их использовать, поэтому он может сойти за мошенника Криса Арагона.

Он начал выбирать оружие, подбирая троянскую программу, которая уже циркулировала онлайн и настраивал, чтобы антивирус ее не обнаруживал. Чтобы

тестировать результаты, он использовал симулятор компьютерного обеспечения VMware, запуская сразу десятки различных виртуальных систем Windows на своём компьютере, каждая загрузка с разным набором программ по безопасности.

Когда вредоносные программы остались незамеченными для других, он приступил к следующему шагу: собрал список номеров от карточек и электронных адресов с публичных форумов, добавляя их тысячами в базу. Затем, представляясь как известный продавец дампов Hummer911, он отправил сообщение для всего списка. В сообщении говорилось, что Hummer911 приобрёл базу дампов American Express больше, чем он мог бы использовать или продать, поэтому он готов часть отдать. «Кликните сюда, — написал Макс, — и получите бесплатный Amex!». Когда владелец карты кликнул по ссылке, то он обнаружил, что смотрит на поддельные дампы Amex. В это время Макс генерирует невидимый код на веб-странице, используя новую уязвимость Internet Explorer.

Эксплоит воспользовался тем, что Internet Explorer может делать больше, чем просто обработка веб-страницы. В 1999 Майкрософт добавил поддержку нового типа файла под названием HTA-приложение. Файл, написанный в той же разметке и языком кодирования, что используется на веб-сайтах, при этом позволяет делать на компьютере пользователя то, что не может делать веб-сайт. Например, создание и удаление файлов по запросу или выполнение произвольных программ. Идея была, чтобы разработчики привыкли к программированию для веба, используя те же навыки, как и при разработке полностью функционального десктопного приложения.

Internet Explorer распознает HTA-приложение, которое может быть смертельно опасным, и не загружает их из сети, а только с жёсткого диска пользователя. В теории. На практике, Майкрософт оставил лазейку на пути сканирования браузером содержания веб-страниц. Многие веб-страницы содержат объектные тэги — простые инструкции, которые говорят браузеру забрать что-нибудь с одного веб-адреса (обычно фильм или музыкальный файл) и включают его в часть страницы. Но оказалось, что вы можете также загрузить HTA-приложение через объектные тэги и получить право на его загрузку. Вам надо только немного замаскировать его.

Пока жертвы Макс радовались поддельным дампам American Express, невидимый объектный тэг управляя их браузером, закачивал вредоносное HTA-приложение, которое Макс, на всякий случай, закодировал.

Важно, что Макс дал файлу имя «.txt» — поверхностный индикатор того, что это обычный текстовый файл. Internet Explorer распознавал имя файла и решал, что его загрузка будет безопасной. Как только браузер начинал загрузку файла, сервер Макса превращал его содержимое в содержимое типа «application/hta», которое

идентифицируется как HTA-приложение. По сути сервер Макса изменял историю загрузки, предлагая безвредный документ для проверки браузером, который определялся как HTA-приложение, в момент, когда браузер обнаруживал файл.

Из-за имени файл сохранялся как безопасный, и Internet Explorer не перепроверял данные, один раз убедившись в них. Он просто запускал HTA-приложение Макса вместо веб-страницы.

HTA-приложение Макса было написано плотным Visual Basic скриптом, который запускался небольшой программой-ловушкой на компьютере пользователя. Макс назвал ловушку «hope.exe». Надежда – это второе имя Черити. Ловушка, в свою очередь, загружала и устанавливала троянского коня. Таким образом у Макса всё было под контролем.

• • •

Кардеры как голодные пираньи собрались на заражённой странице. Сотни машин доложили Максу о готовности к работе на него. Взволнованный, он начал в хаотичном порядке разбираться в преступных жёстких дисках. Он был удивлён тем, как мало времени ушло на это. Большинство его жертв покупали маленькие базы дампов, десять или двадцать за один раз (даже меньше). Там было много кардеров, и ничто не удерживало его от возвращения к их машинам снова и снова. В итоге атака бесплатного Amex принесла ему около десяти тысяч дампов.

Он перекачал дампы Крису, как только нашёл их, и просмотрел другие полезные данные от его жертв: подробности о мошенничествах, украденная личная информация, пароли, e-mail рассылки, где используется фишинг, некоторые реальные имена, фотографии, почта и ICQ номера их друзей – полезных людей для следующих нападений.

С одной хорошо построенной ловушкой, он стал невидимкой, встроенным в систему кардеров. Это было начало чего-то большого. Он будто был главой среди кардеров, живя только за счёт того, что может плавать в их нелегальной экономике. Его жертвы не могли вызвать копов, а с его анонимным соединением с Интернетом и рядом других мер предосторожности, он застрахован от угроз. Это длилось недолго, прежде, чем Макс обнаружил, что не все кардеры были теми, за кого себя выдают. Жертва была в Санта-Анна. Когда Макс начал просматривать компьютер через свой «вход», то сразу понял, что здесь что-то не так.

На компьютере работала программа под названием Camtasia, которая записывала все движения на экране – это обычно не та информация, которую преступник хочет скрыть. Макс проверил жёсткий диск, и его подозрения подтвердились. Диск упакован докладами от ФБР. Крис был потрясен открытиями агента ФБР в области

борьбы с киберпреступлениями – жёсткий диск агента давал потенциально полезные находки о методах ФБР. Они говорили о том, что делать дальше.

В некоторых файлах было указано, что агент имеет информатора, который обеспечивает его информацией про Скрипта. Это был лидер кардеров, который продал Крису его первые дампы. Должны ли они беспокоится, что в кругу Скрипта появился стукач? Они решили ничего не делать. Если они разорятся, Макс подумал, что разыграет этот козырь. Если получится, что он случайно взломал агента ФБР, то это может смутить ФБР, возможно, даже будет стоить нескольких приговоров.

Он вернулся к своей работе по взлому кардеров. Он сейчас знал, что он был не единственным посторонним в мире преступности.

Глава 13. «Вилла Сиена»

У ворот виллы Сиена, обширного жилого комплекса в Ирвине, в полумиле от аэропорта Джона Уэйна, росли пальмы. За главным входом в ухоженных дворах плескались фонтаны в европейском стиле, а четыре бассейна переливались оттенками голубого под солнечным небом южной Калифорнии. Обитатели наслаждались клубом, расслаблялись в спа-салонах, тренировались в одном из трех спортзалов или, быть может, общались с консьерж-менеджером, строя планы на вечер.

В одной из просторных квартир Крис Арагон занимался своим предприятием. Занавески были опущены, чтобы скрыть изобилие техники, заполнившей икеевские столы и гранитные столешницы. Он включил свой принтер для карт, и он пробудился с воющим гулом, колеса завращались, моторы натянули ленты, тугие, как больничные простыни.

Макс теперь вытаскивал дампы регулярно, и, когда он добывал новый трофей, уже нельзя было тратить время — данные были украдены дважды, и Крису приходилось разбираться с ними прежде, чем мошенники, купившие или выкравшие номера, применяли их первыми или же ошибались и вынуждали компании отметить эти карты. Крису пришлось собрать последние сбережения, чтобы вложить около 15 000 долларов в оборудование для печати кредитных карт и квартиру для него.

Теперь вложения стали себя оправдывать.

Он загрузил пустые ПВХ карты в лоток громоздкой продолговатой машины — карточного принтера Fargo HDP600 стоимостью в 5000 долларов, который использовался для печати корпоративных ID. После щелчка мыши на ноутбуке машина втянула карту в свою пасть и прорычала что-то раз, другой, третий, наконец, четвертый. Каждый звук отмечал новый цвет в то время, как пигмент переводился на чистую печатающую ленту и быстро испарялся нагревающим элементом, вплавляясь в поверхность карты. Последний лязг от Fargo сообщал, что прозрачная ламинирующая пленка заняла свое место на пластике.

Сорок четыре секунды от начала до конца — и машина выплевывала карту, блестящую, яркую, настоящее произведение искусства. Это мог быть белоголовый орлан, глубокомысленно таращащийся на логотип Capitol One, или суровый центурион American Express, или простое пятно небесно-голубого на белом фоне для карты MasterCard бренда Sony. Для элитных карт процесс был таким же, разве

что иногда Крис начинал с основ золотого или платинового цвета, которые, как и белые, заказывались сотнями.

Имея колоду свеженапечатаных пластиковых карт, он переходил к второму пункту своего конвеера: черно-белому принтеру для тонкой печати на обороте карты. Если вдруг была нужна голограмма, Крис извлекал из стопки лист китайских подделок, аккуратно помещал под пресс и опускал рычаг, вырезая овал или закругленный прямоугольник размером с марку. Термический штамповщик Kwikprint Model 55 стоимостью в 2000 долларов, напоминающий смесь сверлильного станка и средневекового орудия пыток, вплавлял фольгу в поверхность пластика.

Аппарат для тиснения проводил следующий этап: огромное механизированное колесо с буквами и цифрами, шумевшее, как IBM Selectric, когда выдавливало по букве на пластике имя, номер счета и срок годности, заполняя их серебряной или золотой фольгой. От китайского поставщика Крис узнал специальные ключи безопасности для крылатого V у Визы и объединенного MC МастерКарда — двух отличительных выпуклых знаках, которые можно найти только на кредитных картах, настоящих и поддельных.

Системы верификации не проверяют имени владельца, что давало Крису возможность выбирать для печати на карте любое; для тех, что использовал сам, он предпочитал «Крис Андерсон». На ноутбуке Крис редактировал дампы, полученные от Макса, чтобы имя в магнитной полосе соответствовало тому, что снаружи. Имя не использовалось для вычисления CVV, в отличие от остальных данных на полосе, так что его можно было менять как угодно.

Наконец, два раза проведя карту через верный MSR206, чтобы запрограммировать дамп, Крис получал поддельную кредитку, почти ничем не отличавшуюся от тех, что лежали в карманах и кошельках американских обывателей.

Но это был не конец.

Водительское удостоверение было необходимо для заказов с высоким кредитным лимитом, и тут снова «сборочная линия» Криса и уроки Shadowcrew делали свое дело. Для водительских прав он переходил с ПВХ на Teslin, более тонкий и гибкий пластик продававшийся листами 8x11 дюймов. Один лист на лицо, второй на изнанку, и десять удостоверений на лист.

Калифорнийский вариант прав имел два элемента безопасности, требовавших дополнительных трюков. Первым было полупрозрачное изображение печати штата Калифорния, повторяющееся на лицевой стороне в ламинате. Для подделки Крис

пользовался Pearl Ex, мелким разноцветным порошком, продававшимся в художественных магазинах меньше чем за три доллара банка. Трюк заключался в том, чтобы посыпать лист ламината смесью золотого и серебряного порошка, скормить его принтеру с картриджем с прозрачными чернилами и напечатать зеркальное изображение узора этими чернилами. То, что печать была невидимой, значения не имело, нужно было именно тепло печатающей головки. Лист выходил наружу с узором, вплавленным в поверхность, а лишний порошок легко смывался в холодной воде.

Ультрафиолетовая печать на лицевой стороне была ничуть не более трудным делом. Обычный струйный принтер легко справлялся с работой, если опустошить картриджи и заполнить их разноцветными ультрафиолетовыми чернилами, купленными в тюбиках.

После всех этих процедур у Криса в руках оказывались четыре листа материала. Затем он складывал два листа Teslin между кусками ламината и пропускал этот бутерброд через ламинатор. После того, как карта была вырезана, можно было любоваться впечатляющим результатом: провести пальцами по удостоверению и ощутить гладкую шелковистую поверхность, повертеть в руках и увидеть призрачные печати штата, поместить под ультрафиолетовую лампу и увидеть зловеще светящийся флаг: красные слова «California Republic», а над ними — бурого медведя на желтой вершине холма.

Когда карты и удостоверения были готовы, Крис взял телефон и вызвал своих девушек. Он обнаружил, что привлекательные девушки возраста студенток колледжа лучше всего подходили для обналички. Была Нэнси, девушка латинского происхождения, с татуировкой «love» на запястье, Линдси, бледная брюнетка с карими глазами, Адрианна, молодая итальянка, Джейми, работавшая официанткой в Hooters в Ньюпорт Бич. Кроме них, Крис встретил двух темноволосых близняшек, Лиз и Мишель Эсквер на вилле Сиена, где они жили.

Мишель просто крутилась вокруг группы, а вот Лиз была бесценна: она работала в ипотечной индустрии, обладала острым умом, хорошим образованием и была достаточно ответственна, чтобы поручить ей некоторые административные задачи, такие как ведение таблицы выплат, кроме обычных покупок в магазинах.

У Криса был талант подбирать людей. Он мог встретить новую кандидатку в ресторане и пригласить ее на вечеринку с его друзьями. Тогда она присоединялась к ним в клубах, на дорогих обедах, ездила в дорогих арендованных лимузинах, когда кто-то из них отмечал день рождения. Она видела деньги везде. Когда наступало время, может, когда проходило несколько месяцев, может, когда девушка признавалась, что у нее есть неоплаченные счета или арендная плата, Крис

мимоходом упоминал, что знает способ заработать легко и быстро. Он рассказывал, как это работает, объяснял, что у этого преступления нет жертвы. Иначе девушки привязывали бы это дело к человеку. Никто из них не знал, откуда Крис брал данные кредитных карт. Когда Крис говорил о Максе, то называл его «Свист», и это был таинственный суперхакер, которого они никогда не увидят.

Кодовым именем Криса было «Братан». Теперь, когда операция шла полным ходом, Братан платил Свисту примерно 10000 долларов в месяц за дампы, переводя деньги через предоплаченную дебетную карту Green Dot.

Green Dot от Визы или МастерКарда была разработана специально для студентов и потребителей с плохим благосостоянием, это была кредитка без кредита. Человек оплачивал карту заранее, банковским переводом, зарплатой, наличными. Последнее и делало такую карту идеальным способом перевода денег от Криса в Ориндже и Максом в Сан Франциско. Крис заглядывал в близлежащий 7-Eleven или Walgreens и заказывал номер оплаты Green Dot, называемый MoneyPack, на любую сумму до 500 долларов. Он отправлял Максу номер через IM или электронную почту, а тот использовал его для одной из карт на сайте компании. Макс мог даже пользоваться картой для ежедневных покупок или снимать деньги в банкоматах Сан Франциско.

Как только его команда была в сборе, готовая к работе, Крис раздал им их карты, разделенные на классические, с низким кредитным лимитом, и золотые или платиновые, с высоким. Он напомнил, что с классическими следует придерживаться небольших покупок, примерно 500 долларов. Те, кому достались золотые, должны были совершать покупки покрупнее, от 1000 до 10000 долларов. Девушки были молоды, но под воздействием стильной молодежи Оринджа могли держаться так, что легко входили в Nordstrom и брали пару сумок Coach, не двинув бровью, затем пересекали магазин и повторяли то же в Bloomingdale‘s.

Новички сначала нервничали, но после того, как первая поддельная карта срабатывала на кассе, оказывались на крючке. Вскоре девушки уже слали Крису восторженные сообщения со своих походов по магазинам: «Можно ли пользоваться Amex в новом Bloomingdale‘s?», или «Я сделала 7000 на Мастеркарде! Ура!»

В конце дня они встречались на парковке и передавали покупки из багажника в багажник.

Он платил им на месте, 30 процентов от розничной стоимости, и тщательно записывал каждую выплату, как настоящий бизнесмен. «Элегантная ткань и сверкающие пряжки» сумок оказывались в коробках до тех пор, пока жена Криса, Клара, не продавала их на eBay. На виллу Сиена опустилась ночь, над теннисными кортами включились фонари, зажглись наружные очаги. В милях отсюда команда

отмечала успех хорошим ужином и бутылкой вина. Как всегда, платил Крис.

Глава 14. «Рейд»

«Классный телек!», — сказал Тим, любуясь на 61 дюймовую плазму Sony, висящую на стене. Черити, заядлая любительница чтения, ненавидела этот новый дисплей и то, как он поглотил пространство гостиной в их новом доме. Однако Макс любил свои гаджеты, а этот был больше, чем просто игрушкой. Этот телевизор был символом вновь обретенного финансового благополучия.

Друзья Макса знали, что он чем-то занимается, и не только потому, что ему больше не приходилось еле сводить концы с концами. Макс начал подсовывать Тиму диски с записанными на них свежими эксплойтами, давая таким образом системному администратору преимущество в работе по защите парка машин. Кроме того, имел место его странный комментарий на ежемесячном обеде Голодных Программистов в «Чин-Чин», что в Пало-Альто. Когда все закончили с представлениями своих проектов, Макс смог лишь загадочно, с ноткой зависти, произнести: «Ух ты, вот бы и мне что-то хорошее сделать».

Впрочем, интересоваться подробностями новых занятий у Макса никто не стал. Им оставалось только надеяться, что это будет что-то условно легальное. Хакер, в свою очередь, тщательно старался не обременять друзей информацией о своей двойной жизни, даже когда он окончательно вышел из их круга, но лишь до того момента, пока один из его взломов не привел кое-кого к нему домой.

• • •

Было 6:30 утра, и на улице было еще темно, когда Крис Тошок проснулся от звука его дверного звонка: кто-то долго и настойчиво удерживал палец на кнопке. Решив, что это его пьяный сосед, Крис перевернулся на бок и попытался снова уснуть. Звонок зазвенел вновь, на этот раз прерывисто, подражая сигналу «занято» в телефонной трубке. Крис неохотно выполз из-под одеяла, натянул рубашку и штаны и поплелся вниз. Открыв дверь, Крис тут же прищурился, — кто-то светил ему фонариком прямо в лицо.

— Это Вы Крис Тошок? — Произнес женский голос.

— Мнэээ, да.

— Мистер Тошок, мы из ФБР. У нас есть ордер на обыск вашего дома.

Агент, длинноволосая блондинка, показала Крису свой жетон и всучила ему в руку тонкую стопку бумаг. Другой агент, положив свою твердую руку на плечо

Крису, вывел его во двор, чтобы тот не мешал остальным агентам зайти в дом. Они разбудили соседа Криса, а затем начали обыскивать спальню, перебирая книги на полках и копошась в шкафу с бельем.

Блондинка, сопровождаемая агентом Секретной Службы, присела рядом с Крисом, чтобы объяснить ему, почему они здесь. Четыре месяца назад исходники еще не вышедшего шутера Half-Life 2 были украдены у Valve Software в городе Беллевью, штат Вашингтон. Какое-то время они поболтались по IRC, а затем появились на файлообменниках. Half-Life 2 была, пожалуй, самой ожидаемой игрой всех времен, поэтому появление исходников не на шутку всколыхнуло игровой мир. Valve выступили с заявлением о том, что им придется отложить релиз игры, а глава компании призвал фанатов серии Half-Life помочь выследить вора. Исходя из продаж первой части игры, Valve оценили исходники в 250 000 000 долларов.

Как объяснил агент, отслеживание некоторой хакерской активности привело ФБР прямиком к IP-адресу Тошока, в его старый дом. Поэтому, если Крис хочет смягчить свое наказание, ему придется рассказать, где он хранит исходники.

Тошок заявил о своей невиновности, хотя и сказал, что знал об утечке: его старый друг, Макс Вижн, якобы находился рядом с ним во время всей этой истории, и когда исходники начали появляться в интернете, Крис был очень взволнован. Упоминание имени Макса заставило агентов работать в удвоенном темпе: они торопливо закончили обыск, едва не спотыкались друг об друга, и мигом отправились в офис, чтобы подготовить ордер для обыска нового жилища Макса. Крис мрачно наблюдал за тем, как агенты забирают девять компьютеров, кое-какие музыкальные диски и Xbox. Агент-блондинка заметила выражение его лица и сказала: «Да, для тебя это будет непросто».

Узнав о рейде, Макс понял, что времени у него в обрез. Он бегал по всей квартире, пытаясь припрятать оборудование. Один жесткий диск он зарыл в полотенцах, лежащих в шкафу ванной, другой — в коробке с кукурузными хлопьями. Один из ноутбуков Макс запрятал под диванной подушкой, а второй вывесил за окно в мешке для мусора. Все важное на компьютере было зашифровано, так что даже если бы агенты что-то нашли, они не смогли бы доказать его вину. Однако, по правилам его пребывания на свободе, он не имел права использовать шифрование. Более того, допускать ФБР к его компьютерам было в принципе очень опасно.

Двадцать федералов хлынули в квартиру Макса и расползлись по ней, словно муравьи. Все, что им удалось найти, это несколько обычных атрибутов компьютерного гика с наклонностями хиппи из Сан-Франциско: книжную полку с «1984» Оруэлла, классическим научно-фантастический романом Орсона Скотта

Карда «Игра Эндера» и несколькими произведениями Азимова и Карла Сагана, велосипед и кучу разбросанных повсюду плюшевых пингвинов. Макс любил пингвинов.

Агенты не обнаружили ни одного из наспех сооруженных Максом тайников, так что в этот раз ему не пришлось ничего объяснять. Федералы ушли, не получив ни каких-либо доказательств касательно причастности Макса к утечке из Valve, ни улик относительно преступлений, совершенных им совместно с Крисом. Лишь пачка дисков, сломанный винчестер и старый компьютер с Windows, оставленные на виду для отвлечения внимания.

Зато Черити только что узнала, какого это — быть в мире Макса Вижна. Макс же настаивал на своей непричастности к краже кода. Вероятно, так и было: в ожидании выхода Half-Life 2 вокруг дырявой как швейцарский сыр сети Valve шастали как минимум несколько любителей шутеров, и Макс был лишь одним из них. Позже ФБР взяли в разработку другого хакера: им оказался двадцатилетний немецкий хакер Эксл «Ago» Гембе, который подтверждал свое участие во взломе сети Valve (о чем сам признался в письме главе компании Гейбу Ньюэлу), но отрицал причастность к краже исходников.

Гембе был печально известен благодаря созданию Agobot, продвинутого компьютерного червя, который умел несколько больше, чем распространяться в сетях под Windows. Когда Agobot получал доступ к компьютеру, пользователь мог заметить лишь внезапные «тормоза» в работе системы. Однако в этот момент компьютер жертвы становился частью личной армии хакера. Червь, согласно программе, автоматически входил в определенный IRC-чат, затем объявлял себя и готовился принимать команды, передаваемые хозяином прямо там, в чате. Тысячи компьютеров отвечали на команды, образуя некий улей — ботнет. Одной строчкой кода хакер мог запустить кейлоггеры на удаленных компьютерах, получая пароли и номера кредитных карт. Он мог превратить компьютеры в источники спама. Но хуже всего было то, что этот червь мог заставить все зараженные машины одновременно атаковать потоком трафика любой сайт — такая DDoS-атака могла часами держать в дауне любой топовый веб-ресурс, до тех пор, пока администраторы не забанят каждый из IP-адресов.

Изначально DDoS-атаки были популярны среди хакеров как способ кикнуть друг друга из IRC-чата. Затем, в феврале 2000 года, пятнадцатилетний канадец Майкл «MafiaBoy» Калси в качестве эксперимента натравил свой ботнет на самые посещаемые сайты, которые можно было найти. Сайты CNN, Yahoo!, Amazon, eBay, Dell, E-Trade — все они рухнули под напором, обеспечив газеты громкими заголовками, а экспертов по безопасности в Белом доме — внеочередным экстренным заседанием. С тех пор DDoS-атаки выросли в одну из самых

чудовищных проблем интернета.

Боты как у Гембе стали главной инновацией десятилетия в мире вредоносного ПО, открыв собой новую эру, когда любой озлобленный школьник мог по желанию запросто грохнуть часть интернета. Признание немца во вторжении в сеть Valve дало ФБР шикарную возможность заманить в ловушку одного из самых грешных инноваторов: федералы пытались заманить Гембе в Америку, выслав ему приглашение на работу из самой Valve. После месяцев переговоров и телефонных собеседований с руководителями компании хакер уже был готов прилететь в США, однако в дело вмешалась немецкая полиция и арестовала хакера, осудив его в Германии на срок один год условно.

Прошедший в доме рейд встряхнул Макса, наполнив его голову неприятными воспоминаниями обыска ФБР по подозрению в BIND-атаках. Макс решил, что ему нужен безопасный дом в городе, где он сможет заниматься своей торговлей и хранить данные в недоступном для обысков месте. Например, жилище Криса на Вилле Сиена.

Используя псевдоним, Крис арендовал вторую квартиру, для Макса. Это был просторный пентхаус в районе Fillmore, с балконом и камином. Максу нравилось работать у камина: он шутил, что в случае опасности всегда сможет сжечь улики. Макс пытался бывать дома у Черити каждый день, однако комфортабельное безопасное убежище заставляло хакера пропадать на несколько дней кряду. Появлялся он лишь тогда, когда его подружка отвлекала его от работы телефонным звонком: «Чувак, пора домой. Я скучаю по тебе».

Когда совместная работа Макса и Криса стала приносить деньги, стало появляться и недоверие. Некоторые из барыг в команде Криса любили тусовки, и постоянное присутствие в доме кокаина, экстази и травы действовало на Криса примерно так же, как приходящая на память давно забытая мелодия. В феврале он был задержан за управление автомобилем в нетрезвом виде. В то время он стал регулярно исчезать в Лас-Вегасе со своими миловидными сотрудницами, где пропадал все выходные. Днем они закупались в магазинах, а вечером Крис мог вынюхать пару дорожек и отвезти своих девчонок поразвлечься в «Hard Rock Café» или поторчать за VIP-столиком в елейном баре «Ghostbar» на вершине Палмс, где он мог просадить штуку баксов на обед и еще столько же на бутылку вина. Вернувшись в Оранж Кауинти, он зацепил восемнадцатилетнюю девушку, с которой познакомился через одного из своих барыг.

Максу были неприятны все эти увлечения наркотиками и супружескими изменами. Но что действительно бесило Макса, так это их финансовые договоренности. Крис платил Максу как бог на душу положит: в любой момент он

мог изменить сумму выплат. Макс же хотел стабильные 50 процентов от прибыли Криса. Он был уверен, что Крис поднимает реальные деньги с их совместного дела. Крис попытался объяснить Максу положение дел и отправил ему письмо с описанием доходов и расходов. Согласно ему, из ста карточек срабатывало ну, может, около пятидесяти, и только лишь на половину из них можно было купить что-то ценное; остальные оказывались мусором с лимитом на 500 долларов, которые годились разве что для мелких покупок вроде бензина и еды. Да и у самого Криса были расходы: распространение товара требовало перелетов его команды в отдаленные города, а авиабилеты не дешевели. Кроме того, он платил за аренду помещения в «Вилла Сиена», где находилась его фабрика по производству банковских карт.

Макс же был неумолим: «Позвони мне, когда не будешь обдолбан». Последняя капля в чашу терпения Макса упала три месяца спустя после истории с Half-Life, когда Крис чуть не спалился. Он приехал в Сан-Франциско встретиться с Максом и отоварить карточки в торговом центре Peninsula. Он и его команда как раз расселялись в соседних номерах роскошного отеля «W» в районе Сома, когда Крису позвонили с ресепшена: его кредитка не принималась терминалом. Терзаемый похмельем и гриппом, Крис спустился вниз и достал другую поддельную карточку из своего пухлого кошелька. Он наблюдал за тем, как администратор прокатал его карточку — снова мимо. Крис достал еще одну, но и она была отклонена. Третья карточка сработала, но это вызвало подозрения и, как только лифт отвез Криса на двадцать седьмой этаж, администратор сразу позвонила в банк. Следующими, кто постучался в дверь Криса, были люди из департамента полиции Сан-Франциско.

Надев на Криса наручники, полицейские обыскали его номер и машину, забрав его ноутбук Sony, MSR206 и машину, у которой был перебит VIN: в Лас-Вегасе Крис экспериментировал с арендованными на поддельные карточки машинами, отправляя тачки в Мексику, где они получали новые номера.

Криса упекли в окружную тюрьму. Его исчезновение обеспокоило Макса, но Крис легко отделался и признал перед партнером свою ошибку. К счастью для него, полицейское расследование далеко не ушло. Месяц спустя Крису дали три года условно и запретили посещать отель «W». После этого он еще хвастался, что стал, так сказать, бенефициаром системы правосудия Сан-Франциско.

Примерно та же самая фигня регулярно случалась с девочками Криса, поэтому он держал на зарплате поручителя и даже позволял ему ночевать на своей подпольной фабрике карточек в «Вилла Сиена». Но Макс был взбешен. Для человека уровня Криса позволить поймать себя в номере гостиницы за кардинг — непростительная небрежность.

Макс решил, что он больше не может полагаться на своего партнера. Ему был нужен план «Б».

Глава 15. «UBuyWeRush»

Захудалый торговый центр был расположен в том обширном равнинном интерьере Лос-Анджелеса, который вряд ли бы напечатали на открытке. Далеко от океана и так далеко от холмов, что приземистые оштукатуренные строения могли бы стать Голливудской сценой, где невыразительное голубое небо за ними играло бы роль хромакея, который заполнят горами или деревьями во время пост-продакшна.

Крис припарковал машину на стоянке усеянной мусором. На маркизе перед входом верхняя вывеска рекламировала салун «Страна ковбоев», ниже шел обычный для юга Лос-Анджелеса набор: винный магазин, ломбард, маникюрный салон. Еще одна была не совсем обычной: UBuyWeRush (ТыПокупаешьМыСпешим) — единственная магазинная вывеска в Лос-Анджелесе, которая так же являлась ником на сайтах CarderPlanet и Shadowcrew.

Он прошел внутрь офиса, где пустое окно ресепшна предлагало в аренду помещения бывшей медицинской клиники по 60 центов за квадратный метр. На стене висела карта мира в проекции Меркатора ощетиненная канцелярскими кнопками. Криса тепло встретил лично UBuy — Цезарь Карренза.

Цезарь пришел в подполье окольным путем. В 2001 году он закончил институт DeVry по специальности программирование и надеялся найти работу в Интернете. Когда найти такую не удалось, он решил попробовать себя в качестве самостоятельного предпринимателя в сети.

Из объявления в газете Daily Commerce он узнал о предстоящем аукционе, где владельцы публичного склада в Лонг Бич продают содержимое контейнеров, брошенных арендаторами. Придя на этот аукцион, он обнаружил, что там соблюдается весьма специфический ритуал. Управляющий, вооружившись внушительным болторезом, перерезал замок недобросовестного владельца на глазах у участников аукциона и открывал дверь. Участники — их было около двадцати — старались оценить содержимое стоя на отдалении нескольких метров. Победитель мог закрыть контейнер своим навесным замком и должен был очистить его от содержимого в течение 24-х часов.

Опытных участников аукциона было легко определить по свисающим с их поясов замкам и фонарикам, чтобы вглядываться в темные контейнеры. Цезарь не был так подготовлен, но был полон энтузиазма. Он был единственным, кто сделал ставку на первый лот аукциона, заполучив за 1 доллар контейнер полный старой одежды.

Он продал одежду на гаражной распродаже и на eBay на сумму около 60 долларов. Осознавая, что он нашел неплохую нишу, Цезарь стал посещать больше аукционов на складах и ликвидациях бизнесов подламывая большие лоты и реализовывая их на eBay с довольно неплохой прибылью. Он вкладывал полученные деньги обратно в бизнес и открыл собственную витрину в торговом центре Лонг Бич, чтобы принимать товары от соседей: офисную мебель, шезлонги, джинсы неизвестных производителей, и продавать их онлайн.

Это была хорошая, честная работа — не то, что его последний бизнес. На протяжении большинства лет в 90-х, Цезарь занимался мошенничеством с кредитными картами. Он был гораздо счастливее сейчас, когда занимался продажами через eBay, но воспоминания о прошлом заставили его задуматься: что если бы существовал специализированный магазин оборудования, которое он использовал, как мошенник. Он заказал несколько MSR206 у производителя и разместил их в своем магазине UBuyWeRush на eBay. Он был впечатлен тем, как быстро их расхватали.

Один из его новых покупателей рассказал ему о сайтах, где он действительно мог продавать. Он представил Цезаря Скрипту, который утвердил UBuyWeRush в качестве продавца на CarderPlanet. Цезарь разместил свое вступительное слово 8 августа 2003: «Я решил обеспечить всем необходимым всех вас, ребята, кто делает действительно много баксов» — написал он. «Так что если я вам нужен, я продаю принтеры для карт, эмбоссеры, типперы, кодировщики, небольшие считыватели и прочее. Я знаю, это звучит как реклама, но это для вас, БЕЗОПАСНОЕ место для покупок».

Бизнес взлетел той же ночью. Цезарь создал собственный сайт, начал торговать на Shadowcrew, получил телефонный номер 800 и стал принимать e-gold — излюбленную анонимную онлайн-валюту кардеров. Он заслужил репутацию за отличный клиентский сервис. С клиентами любого часового пояса он был очень щепетилен и отвечал на телефонные звонки когда бы они не случались — днем или ночью. На другом конце провода всегда были деньги.

Будучи ответственным бизнесменом, он гарантировал отправку в день заказа и выстраивал отношения со своими конкурентами, так что если вдруг у него образовывался дефицит одного из товаров, он мог пополнить запасы у конкурента, чтобы выполнить заказы и оставить своего покупателя довольным. Подобные стратегические ходы скоро сделали UBuyWeRush топовым поставщиком оборудования для хакеров и похитителей персональных данных по всему миру.

«Действительно хороший человек, с которым приятно иметь дело», — написал кардер, именующий себя Страх, консультируя новичка сайта Shadowcrew. — «Не

кидай UBuyWeRush, потому что он классный парень и будет держать информацию о тебе в тайне».

Скоро Цезарь расширил ассортимент на сотни единиц: скиммеры, специальные камеры для фото на документы, прессы для тиснения фольгой, чистый пластик, принтеры для печати штрих-кодов, эмбоссеры, чековая бумага, картриджи с магнитными чернилами, даже дешифраторы для кабельного ТВ. Торговля оборудованием сама по себе была законной до тех пор, пока он не использовал его в криминальных целях. У него были даже законопослушные клиенты, которые покупали его технику для изготовления удостоверений компании и школьных талонов на обед.

Заваленный заказами, Цезарь дал объявление о поиске помощников в соответствующий раздел и начал нанимать работников для ведения учета, упаковки и отправки товаров. Когда открылись помещения по соседству, он присоединил их в качестве дополнительного склада, удвоив, а затем утроив его площадь. Зачарованный глобальным охватом своего скромного магазинчика, он купил настенную карту и, каждый раз отправляя заказ в новый город, втыкал кнопку в место отправки. Через полгода карта была утыкана кнопками, подобно дикобразу, по всем Соединенным Штатам, Канаде, Европе, Африке и Азии. Непроходимый лес из металла на карте вырос юго-западнее России на Черном море. На Украине.

Крис и Цезарь стали друзьями. Он даже пригласил его на обед вместе с Миссис UBuyWeRush — Кларой, а так же двумя сыновьями Криса — хорошо воспитанными детьми, которые остались за столом до самого десерта. Крис особенно любил зависать в офисе Цезаря. Никогда не знаешь кто придет в UBuyWeRush. Кардеры слишком параноидальны, чтобы заказывать доставку нелегального оборудования даже на подставное лицо, поэтому в большинстве случаев были готовы совершить путешествие в Лос-Анджелес и забирать свои вещи лично, открывая дверь рукавом рубашки, чтобы не оставлять отпечатков пальцев, и платили наличными. Иностранные кардеры отдыхающие в Калифорнии заезжали просто чтобы увидеть легендарный склад собственными глазами и пожать руку Цезарю.

В тот день человек, зашедший забрать MSR206 был последним, кого Крис ожидал увидеть в магазине Цезаря — двухметрового хакера с длинными волосами, собранными в хвост.

Крис был потрясен. Макс редко покидал Сан-Франциско в последнее время, и он ничего не говорил о том, что собирается выбраться в город. Макс был так же удивлен, увидев Криса. Они неуклюже обменялись любезностями.

Была только одна причина, которая заставила бы Макса тайно выбраться в Лос-Анджелес для покупки персонального кодировщика магнитной полосы — Крис это знал. Макс решил прекратить делиться наиболее ценными данными.

— Макс приложил руку к одной из самых крупных ошибок безопасности в банковской истории, той, о которой большинство потребителей никогда бы не услышали, в то время, как она обогащала кардеров на суммы в миллионы долларов.

Commerce Bank — банк средних размеров в Канзас-Сити, штат Миссури — возможно, был первым, кто понял, что происходит. В 2003 году банковский управляющий безопасностью был предупрежден о необходимости проверить клиентские счета, с которых в течение дня были сняты суммы от 10 до 20 тысяч долларов через банкоматы в Италии — он придет в понедельник и обнаружит, что его банк потерял 70 тысяч долларов за выходные. Когда он провел расследование, он понял, что пострадавшие клиенты стали жертвами фишинговых атак, направленных конкретно на похищение номеров и PIN-кодов их дебетовых карт.

Но кое-что в этой истории не имело смысла: коды CVV должны были предотвратить такой вид мошенничества. Без CVV кода безопасности, хранящегося на магнитной полосе карты, украденная при помощи фишинга информация не должна была сработать ни на одном банкомате в мире.

Он копнул глубже и выяснил правду: его банк просто не проверял CVV коды ни в банкоматах, ни при покупках по дебетовым картам, где покупатель вводит PIN для авторизации. На самом деле, банк не мог проводить подобную проверку, даже если бы захотел — сторонняя процессинговая сеть используемая банком даже не передавала секретный код. Итальянские фишеры могли внести любую бессмыслицу в поле CVV и карта была бы принята, как валидная.

Управляющий сменил процессинговую сеть и перепрограммировал сервер на верификацию CVV. Таинственные выводы денег из Италии прекратились той же ночью.

Но Commerce Bank банк был только началом. В 2004 году примерно половина американских банков, кредитно-сберегательных организаций и кредитных союзов все еще не заботились о верификации CVV в банкоматах и при дебетовых транзакциях, поэтому папки входящих сообщений полнились фишинговыми письмами нацеленными на PIN-коды банков, которые кардеры называли «обналичиваемыми».

Citibank — крупнейший национальный банк по размеру вкладов — был самой известной жертвой. «Это сообщение было отправлено сервером Citibank, чтобы уточнить Ваш адрес электронной почты» — можно было прочитать в сообщении из

России во время сентябрьской кампании 2003 года — «Вы должны завершить этот процесс, нажав на ссылку ниже и указав в появившемся маленьком окне Ваш номер карты Citibank и PIN, который Вы используете в банкомате.»

Более творческие сообщения в 2004 использовали обоснованные страхи клиентов перед кибер-преступлениями. «Не так давно произошло большое количество попыток кражи персональных данных направленных на клиентов Citibank», — гласило сообщение, украшенное логотипом Citibank. — «Для того, чтобы обезопасить Ваш счет, мы просим Вас обновить PIN вашей карты Citibank». Нажав на ссылку, клиент банка попадал на отлично подготовленное подобие оригинального сайта, размещенное на хостинге в Китае, где жертве предлагалось ввести данные.

Отлично подходившие для прямого снятия наличности, PIN-коды были святым Граалем кардинга. И был Король Артур (King Arthur) с сайта CarderPlanet, который был наиболее успешен в его поиске. Король, как его звали друзья, руководил интернациональной сетью, специализировавшейся по атакам на клиентов Citibank. Он был легендой в мире кардинга. Один из заместителей Короля Артура, американский экспат в Англии, однажды обмолвился коллеге, что Король делает 1 миллион долларов в неделю на международных операциях. И он был лишь одним из многих выходцев из Восточной Европы занимавшихся обналичиванием в Америке.

Макс включился в историю с Citibank по своему: он заразил трояном американского обнальщика под ником Такс (Tux) и начал перехватывать PIN-коды и номера счетов, которые тот получал от своего поставщика. Через некоторое время, он связался с источником поставок — анонимным Восточно-Европейцем, за личностью которого, как подозревал Макс, скрывался сам Король Артур — и откровенно признался ему в том, что сделал: он сказал, что Такс был виновен в безалаберном отношении к безопасности. Для верности, Макс добавил безосновательное обвинение обнальщика в обкрадывании своего поставщика.

Поставщик сразу же прекратил отношения с Таксом и начал пересылать PIN-коды напрямую ему, признав хакера своим новым обнальщиком. Когда PIN-коды начали поступать, Макс передавал их Крису, который вгрызался в них со всей силы. Крис снимал 2000 долларов наличными — дневной лимит банкоматов — затем посылал девочек совершать покупки в магазинах до полного опустошения счета. Он потрошил карты. Максу это не нравилось. Весь смысл обналичивания был в получении наличных, а не в перепродаже вещей лишь за часть их стоимости. Добавив в схему немного изящества, можно было сделать карты более ликвидными.

Затем ему пришло в голову, что он вовсе не нуждается в своем партнере для этих конкретных операций.

Вернувшись от UBuyWeRush со своим собственным MSR206, Макс начал вести бизнес самостоятельно. Он кодировал пачку подарочных карт Visa информацией по счетам и писал на прикрепленной к каждой карте бумажке ее PIN. Затем он садился на велосипед или шел пешком по извилистому пути через весь город посещая небольшие частные банкоматы расположенные в местах недоступных камерам наблюдения. Он вводил PIN, сумму снятия и клац, клац, клац, клац — банкомат выдавал наличные, как игровой автомат в казино. Макс убирал деньги, записывал на листочке новый баланс счета карты, оглядывался, чтобы убедиться, что не привлек лишнего внимания, и доставал следующую карту из набора. Чтобы не оставлять отпечатков пальцев, он нажимал кнопки через кусочек бумаги или ногтями, либо покрывал кончики пальцев гидроксиквинолином — прозрачным липким антисептиком, который продавался в аптеках в качестве жидкого пластыря.

Макс исправно отправлял процент своей выручки в Россию через систему MoneyGram компании Western Union, согласно их договору с поставщиком. Теперь он на самом деле был преступником и занимался однозначно подпольным бизнесом. Даже после того, как обзавелся собственным кодировщиком, Макс продолжал отдавать некоторые PIN-коды Крису, который продолжал заставлять свою команду агрессивно выжимать счета до конца.

Понятно, что промысел Макса не особо походил на деятельность Робин Гуда, но Макс испытывал моральное утешение от того факта, что обналичивание всегда заканчивалось блокировкой карты. Это означало, что мошеннические снятия наличных были обнаружены и Citibank будет вынужден возместить потери своих клиентов от воров.

Через несколько месяцев Макс неплохо устроился на потерях Citibank: он вместе с Чарити переехал в дом стоимостью 6000$/мес. в Коул Велли, Сан-Франциско, и установил сейф для полученных доходов в 250 000 долларов наличными.

Его прибыль была лишь мелкой частью всех потерь от оплошности с CVV-кодами. В мае 2005 аналитики компании Gartner провели опрос 5000 онлайн-потребителей и, экстраполировав результаты, подытожили: эта ошибка стоила финансовым институтам США 2.5 миллиарда долларов. Всего за 1 год.

Глава 16. «Операция Фаервол»

Что-то странное происходило с ShadowCrew.

Макс старался не светиться на одном из самых криминальных сайтов во всем интернете. Для него ShadowCrew была лишь площадкой, где можно было взломать пару-тройку кардеров. Однако, в мае 2004 года, администратор сайта сделал заявление, которое привлекло внимание Макса. Админ Cumbajohnny представил новый VPN сервис только для участников сайта.

VPN — виртуальная частная сеть, используется для обеспечения удаленного доступа к сети поверх другой сети. Например, доступ сотрудника из дома к офисной сети компании. Но основной причиной появления VPN сервиса стала возможность шифрования данных, передаваемых через эти сети. Для подполья это был идеальный вариант, чтобы обезопасить свои сделки от любопытных провайдеров или правоохранительных органов, так как любые попытки отследить криминальную деятельность закончатся там же, где начнутся.

Cumbajohnny был последним прибавлением в руководстве, — бывший модератор быстро поднялся в иерархии сайта и стал иметь влияние на настроение форума. Другие админы даже отметили увеличение активности пользователей на форуме. Наверху сайта висели баннеры: «Хватит болтать, делай деньги. Размещай рекламу здесь. Свяжись с Cumbajohnny.» ShadowCrew стал похож на вывеску в Лас-Вегасе: вспыхивающие баннеры, обещающие вечную вечеринку, женщин и кучу денег.

Gollumfun, известный основатель, публично заявил о своем уходе от дел ShadowCrew, когда другой основатель BlackOps также собрался уходить. Он написал: «Будучи прекрасной площадкой, ShadowCrew унизительно пал в окружении детей, которые не ценят знания, навыки и общение с другими членами сайта в позитивном ключе. Сгинули те продуманные тьюториалы, исчезли многоуважаемые пользователи, исчезла цивилизация. Мы больше не будем помогать новичкам искать их призвание, отныне мы будем позорить их, пока они не уйдут с сайта, пока не поймут, что новых пользователей нет и не будет. BlackOps, тебя будет не хватать. Спасибо за твой вклад.» Cumbajohnny ответил весьма кратко: «ShadowCrew меняется. Это к лучшему.»

Макса не особо заинтересовали перемены на политической арене сайта, но появление VPN его весьма озадачило. Оказалось, что Cumbajohnny продавал услуги его личной VPN верхушке ShadowCrew в течение трех месяцев. Теперь же Cumbajohnny писал, что любой член ShadowCrew, не имеющий штрафов, может

купить кусочек спокойствия за 30-50 долларов в месяц.

Однако хорошо известно, что VPN сети имеют одно слабое место — все, что передается по сети, проходит через центральную точку в незашифрованном и уязвимом виде. Как заметил один из участников форума: «Если ФБР или кто-то, кому очень нужно получить данные, попадет в датацентр и изменит некоторые настройки VPN сервера, то пользователям этого сервера придется несладко.» «Но это просто паранойя». — признался он.

Cumbajohnny поспешил его успокоить: «Никто не сможет ковыряться в VPN без моего ведома».

Максу эти сообщения показались не убедительными. Будучи белой шляпой, он как-то он писал программу для проекта Honeynet, называемую Privmsg. Это был скрипт на PERL, который брал данные из сниффера пакетов данных и восстанавливал на их основе IRC-чат. Когда злоумышленник начинал взлом одной из ловушек honeypot‘a, он старался поддерживать связь с другими хакерами. Посредством программы Макса PRIVMSG специалисты могли видеть всю эту переписку. Это было сильным прорывом в борьбе с хакерами, превращая пассивные honeypot‘ы в мощные ловушки, проливая свет на мотивы и культуру подполья.

В данный момент Макс наблюдал ту же картину с перехватом данных в предложении Cumbajohnny. Были и другие причины подозревать Cumbajohnny. Как-то, взламывая случайных кардеров, Макс увидел сообщение, отправленное администратору ShadowCrew, которое выглядело как инструкция для информатора федерального агентства. Что-то подсказывало Максу, что изменения с ShadowCrew превратили сайт в новый Honeypot. После обсуждения своих догадок с Крисом Макс запостил несколько сообщений на форуме, высказав свои подозрения. Сообщения исчезли сразу же. Подозрения Макса подтвердились.

Полиция Нью-Йорка поймала Альберта Cumbajohnny Гонзалеса девять месяцев назад, когда он снимал деньги в банкомате на Uper West Side. Родом из Майами, Гонзалес был 21 летним сыном двух кубинских иммигрантов. Долгое время он занимался взломами, решившись однажды посетить Def Con в Вегасе в 2001 году. Общаясь с Гонзалесом в заключении, Секретная Служба быстро сообразили о полезности Cumbajohnny. Альберт жил садовом домике Кирни за 700 долларов в месяц, имел долг в 12000 долларов и официально числился безработным. Но как Cumbajohnny он был доверенным лицом и коллегой у кардеров по всему свету и, что самое главное, модератором в ShadowCrew. Он был в логове зверя и, подготовившись должным образом, он мог нанести сокрушительный удар по форуму.

Под свою ответственность Секретная Служба освободила Гонзалеса и стала использовать его в качестве информатора. VPN была мастерским трюком агенства. Оборудование было куплено и оплачено федералами, и они же получили ордеры на перехват данных всех пользователей сайта. Cumbajohnny всего лишь приглашал кардеров на этот паноптикум.

Крупные игроки ShadowCrew сразу же попали под наблюдение Секретной Службы. Дырявая VPN обнажила весь процесс кардинга, который до этого оставался в тени — жесткие переговоры, которые велись посредством электронной почты и мессенджеров.

Каждый день и каждую ночь проводились какие-либо сделки, со всплеском торговли по воскресным вечерам. Сделки варьировались от маленьких до гигантских. 19 мая агенты наблюдали за трансфером Скарфейса и другим членом сайта на 115695 кредитных карт; в июле АПК передал поддельный Британский паспорт; в августе Mintfloss продал поддельные Нью-Йоркские водительские права, карточку медицинской страховки и студенческий билет городского университета Нью-Йорка человеку, который запросил полный набор документов. Несколько дней спустя прошла еще одна сделка Скарфейса — в этот раз всего две кредитки; после МАЛпадре купил сразу девять. В сентябре Дэк продал свои наработки в виде базы 18 миллионов взломанных e-mail адресов, которые содержали имя, пароли и даты рождения пользователей.

На Секретную Службу работало пятьдесят агентов, которые отслеживали каждую транзакцию на сайте, подготавливая обвинительную базу. Однако, хуже всего было то, что большая часть обитателей ShadowCrew платила за то, чтобы их отслеживали агенты Секретной Службы.

Вскоре агенты узнали, что в их, казалось бы, продуманной операции против хакеров, были пробелы. 28 июля 2004 года Гонзалес сообщил своим нанимателям, что кардер под ником Myth, один из кешеров Короля Артура, каким-то образом раздобыл один из секретных документов Агентства, в котором описывалась операция Фаервол. Myth сразу же похвастался этой новостью в IRC-руме.

Федералы приказали Гонзалесу как можно быстрее найти источник утечки. Гонзалес связался с Myth под своим ником и узнал, что озвученные документы лишь капля в море утекших данных Секретной Службы. Myth также рассказал, что в отношении ShadowCrew велось уголовное дело, рассказал даже о том, что агентство имело свой ICQ аккаунт.

К счастью для Гонзалеса, в документах не упоминалось об информаторе. Myth отказался выдавать Гонзалесу свой источник, но согласился организовать встречу.

На следующий день Гонзалес, Myth и таинственный хакер, использовавший временный ник «Anonyman», встретились в IRC. Гонзалес старался изо-всех сил, чтобы заслужить доверие Anonyman, прежде чем хакер раскрыл свою личность.

Это был Ethics, поставщик, которого Cumbajohnny уже знал по работе на ShadowCrew. Утечка начинала обретать очертания. В марте Секретная Служба замечала, что Ethics продавал доступ к базе данных крупного оператора сотовой связи T-mobile. Он писал на форуме: «Я предлагаю доступ к информации о клиенте по номеру оператора T-Mobile. Как минимум вы получите имя, номер социального страхования и дату рождения клиента. Как максимум вы получите логин и пароль для выхода в интернет, пароль голосовой почты и секретный вопрос/ответ.»

T-Mobile не смогли исправить критическую брешь в защите приложения сервера, которое было куплено в Сан-Хосе у компании БЕА Системс. Дыра, которую обнаружили сторонние исследователями, была до обидного проста для использования — недокументированная функция позволяла удалять или изменять файлы в системе путем подачи специального веб-запроса. БЕА выпустила патч для этого бага в марте 2003 года и присвоила ему рейтинг высокой опасности. В июле того же года исследователи, которые обнаружили дыру, выступили с докладом на Сборе Black Hat в Вегасе по поводу этого бага. Таким образом, пре-Def Con собрала 1700 специалистов в области защиты информации и руководителей корпораций, дала новый виток информации о бреши в защите T-Mobile.

Ethics узнал о дыре БЕА, написал 21 эксплоит на Visual Basic и начал сканировать интернет на наличие потенциальных жертв, кто не смог или забыл пропатчить приложения. К октябрю 2003 года он окунул T-Mobile в грязь. Ethics написал приложение, при помощи которого мог в любой момент обращаться к базе клиентов.

Для начала он использовал свой доступ для получения данных звезд Голливуда. Ему удалось получить откровенные фото Пэрис Хилтон, Деми Мур, Эштона Катчера и Николь Ричи, украденные из их коммуникаторов. Теперь было очевидно, что скоро и он станет помощником Секретной Службы.

Простой поиск в гугле по ICQ номеру Ethics выдал его настоящие имя, указанное в резюме 2001 года при поиске работы в сфере компьютерной безопасности. Это был Николас Якобсен, 21 летний орегонец, который переехал в Ирвин, штат Калифорния, чтобы работать сисадмином. Все, что нужно было Секретной Службе для предъявления обвинений Якобсену, — важная информация на его коммуникаторе.

Здесь Гонзалес снова показал себя во всей красе. Теперь, будучи в приятельских

отношениях с Cumbajohnny, Ethics заинтересовался VPN сервисом лидера ShadowCrew, объясняя это тем, что при помощи виртуальной сети он сможет безопаснее использовать базу T-Mobile. Гонзалес с радостью согласился помочь, и его хозяева из Секретной Службы начали наблюдать, потирая руки, как Ethics бродит по базе данных T-Mobile, используя логин и пароль агента Петра Кавиччиа III, ветерана борьбы с киберпреступностью, который прославился благодаря аресту сотрудника AOL, на краже 92 миллионов e-mail‘ов клиентов для продажи спаммерам.

Утечка была найдена. Кавиччиа спокойно ушел в отставку три месяца спустя, а Ethics был добавлен список целей операции «FireWall». Была еще одна угроза расследованию и, как ни странно, исходила она от одного из активов ФБР.

Дэвид Томас — мошенник по жизни, обнаружил криминальный форум в Фальшивой библиотеке и вскоре стал одним из жуликов в криминальном сообществе. Теперь 44 летний Эль Мариачи, как он себя называл, был одним из самых уважаемых членов в сообществе кардеров, взяв на себя роль наставника для молодых мошеников, раздавая советы на все случаи, начиная кражей личных данных и заканчивая уроками жизни, которые он получил, живя на окраине.

Однако его опыт не помог ему избежать опасностей его профессии. В октябре 2002 года Томас показался в парке возле офиса в Исаква, штата Вашингтон, где он и его напарник арендовали убежище для одного из основателей CarderPlanet. Они надеялись получить 30 000 долларов товарами в Outpost.com по заказу Украинца. Но вместо этого их ждала местная полиция.

Арестовав Томаса, детектив зачитал ему его права и дал ему бумагу для подписи, подтверждающей, что он их понял. От одной мысли о том, что местный коп пытается допросить его, Томас рассмеялся. «Вы не знаете, кого вы взяли». Томас просил детектива позвонить федералам. Секретная служба должна была знать, кто такой Эль Мариачи, который может дать им дело о русских и «миллионах долларов».

Секретная Служба навестила его в окружной тюрьме, но не была впечатлена его бизнесом на 30 000 долларов. Затем появился агент из местного отделения ФБР в Сиэтле. На вторую встречу агент привез с собой помощника прокурора США и предложение — федералы не могут помочь Томасу в его местном аресте, но когда Томас выйдет из тюрьмы, он сможет работать в Северо-Западной целевой группе по расследованию кибер-преступлений.

Это была бы разведывательная миссия, официальное название для операции ФБР без предварительных целей. Бюро выделило бы Томасу новый компьютер, поселило

бы его в роскошных апартаментах, оплачивало бы все его расходы и давало 1000 долларов в месяц на карманные расходы. Взамен Томас должен был собирать информацию о подполье и сообщать все новости целевой группе.

Томас ненавидел стукачей, но ему нравилась идея получать деньги за возможность наблюдения и комментирования подполья, которым он был одержим. Однако сбор информации это не доносительство, так он считал. Он мог использовать материал, который соберет, чтобы написать книгу о кардинге, о чем-то, о чем он думал очень много в последнее время.

Также он определенно знал, как собирать информацию и о самой целевой группе.

Томас вышел из тюрьмы спустя пять месяцев после ареста. А в апреле ФБР получило новый актив в войне с киберпреступностью — Эль Мариачи и его совершенно новый, финансируемый государством форум, названный Grifters (Кидалы).

Живя на проплаченой бюро квартире в Сиэтле, Томас очень скоро собрал достаточно информации о его братьях-кардерах, в особенности из Восточной Европы. Хоть Томаси работал на ФБР, не ощущал родства с другими государственными органами, и появление новостей о VPN сервисе подсказало ему верно — Cumbajohnny был информатором федералов.

Томас зациклился на разоблачении его конкурента. Игнорируя предписания его куратора из ФБР, он постоянно выкрикивал имя Гонзалес на форумах. Гонзалес тоже в долгу не оставался, он нашел копию полицейского отчета об аресте Томаса и разослал ее кардерам Восточной Европы, обращая внимания на строки, где Томас предлагал помощь в поимке русских. Из-за войны двух информаторов началась масштабная война между ФБР и Секретной Службой.

Это было неподходящее время для недовольства западных европейцев американской драмой кардеров. В мае 2004 года один из украинских основателей CarderPlanet был экстрадирован в США после ареста на отдыхе в Тайланде. В следующем месяце Британская национальная полиция переехал в Лидс, на сайт для англоязычных администраторов.

Скрипт, которого допекало ФБР из округа Орандж и Американская почтовая инспекция, смылся с сайта, оставив во главе Короля Артура. 28 июля 2004 года Король сделал заявление.

Он написал: «Пришло время сообщить вам плохие новости — форум должен быть закрыт.» «Да, это действительно означает закрытие и тому есть много причин.»

На ломаном английском он объяснил, что CarderPlanet стал магнитом для правоохранительных органов со всего света. Когда кардеры попадались, полиция выбивала из них факты о форуме и его лидерах. Под постоянным давлением он мог ошибаться. «Мы все просто люди и каждый из нас может совершать ошибки.»

Закрыв сайт CarderPlanet, он лишит его врагов самого жирного куска.

«Наш форум хорошо их подготовил, постоянно держа в форме и сообщая обо всех новинках в мире подполья. Теперь всё будет одинаковым. Они не будут знать, откуда дует ветер и что с ним делать», — сказал Артур.

С этой прощальной речью Король Артур, десятикратный миллионер, стал легендой кардеров. Его будут помнить как человека, который аккуратно вынашивал великий CarderPlanet прежде, чем кто-либо другой смог получить удовольствия от его разрушения.

Лидерам ShadowCrew повезло меньше. В сентябре ФБР махнуло рукой на операцию с Томасом и дало ему месяц для выезда с квартиры и завершения его войны с Cumbajohnny. В следующем месяце, 26 октября, шестнадцать агентов Секретной Службы собрались в командном центре Вашингтона, готовые начать Операцию «FireWall». Их цели были отмечены на карте США, заполняющей экраны компьютеров. Агенты знали, что каждая их жертва должны быть дома, — по приказу Секретной Службы Гонзалес назначил онлайн встречу на этот вечер, и никто не отказал Cumbajohnny.

В девять вечера агенты, вооруженные полуавтоматическими MP5 ворвались в дома членов ShadowCrew, схватив трех основателей, хакера Ethics и шестнадцать других покупателей и продавцов. Это была самая большая облава на воров в американской истории. Два дня спустя федеральное жюри вынесло шестьдесят два обвинительных приговора, а Министерство Юстиции выступило перед публикой с информацией об Операции «FireWall».

«Этот приговор поразил самое сердце организации, которая позиционировала себя как универсальный рынок для воров персональных данных», — хвастался прокурор Джон Эшкрофт. «Министерство юстиции стремится ловить тех, кто занимается кражей или мошенничеством с данными независимо от того, в интернете они или нет.»

С помощью Гонзалеса Секретная Служба заблокировала оставшиеся 4000 пользователей сайта и заменило домашнюю страницу на баннер Секретной Службы в виде решетки. Новая страница содержала новый слоган «Вы больше не анонимны!!»

В панике кардеры по всему миру начали читать новости и смотреть телевизор в поисках информации, так как были обеспокоены за свое будущее и за будущее земляков. Они собрались на маленьком форуме, названном Стелс Дивижн, чтобы оценить ущерб и принять оставшихся. «Я боюсь до смерти за мою семью, за моих детей», — написал один из кибер-преступников. «Я только что осознал, что каждый мой шаг отслеживался».

Постепенно оставшиеся участники сайта поняли, что Cumbajohnny не был в списке обвиняемых. Вот тогда-то он и появился в сети, чтобы сделать финальное заявление.

«Я хочу, чтобы каждый знал, что я в бегах и я не имею ни малейшего представления, откуда у Секретной Службы США была возможность сделать то, что они сделали. Из новостей я узнал, что они получили доступ к VPN и к ShadowCrew. Это мой последний пост, удачи.»

Ник Якобсен, Ethics, не был допущен к пресс-релизу и удерживался в Лос-Анджелесе. После того, как агентство собрало все награды за Операцию «FireWall», Ethics было предъявлено обвинение за взлом электронной почты Секретной Службы. И все равно это была чистая победа для правительства. CarderPlanet был закрыт, ShadowCrew закрыт навсегда, их лидеры, кроме Гонзалеса, в тюрьме.

Кардеры были ошарашены, обессилены и на данный момент лишены убежища. «Уйдут десятки лет, чтобы в интернете появилось нечто, подобное ShadowCrew. И даже если такое появится, сила правосудия снова победит это. А зная, какая расплата последует за этим преступлением, я сомневаюсь, что кто-то рискнет начать новое дело.»

Глава 17. «Пицца и Пластик»

На верхнем этаже небоскреба на Post Street, на полу из ламината, стоял компьютер Макса — тихий и холодный. Это была маленькая квартира, размером чуть больше тюремной камеры. Эту квартиру нашел ему Крис, и она соответствовала всем его запросам: маленькая площадь, огромное количество соседских Wi-fi сетей. Квартира была декорирована под светлое дерево, в ней стоял большой холодильник и была кровать-раскладушка, которая убиралась в стену.

Это была чистенькая квартирка площадью в 27 квадратных метров без каких-либо излишеств, где Макс скрывался после того как оставил свой пентхаус. Он получил неплохой навар после операции с Citibank и не занимался взломами уже несколько месяцев. Крису оставалось лишь приготовить поддельные документы для полугодовой аренды квартиры и заплатить депозит в размере 500$.

За окном виднелись магазины и квартиры, которые, сами того не зная, уже были готовы предоставить компьютеру Макса канал для связи. Как только его компьютеры были включены, а антенна поймала канал какого-то простофили, Макс потратил немного времени, чтобы вернуться к своим делам.

Как обычно он нацеливался на фродеров и для этого он разработал несколько новых методов кражи данных. Он был в курсе последних фишинговых атак, так как мониторил оповещения от организации под APWG (Анти-Фишинговая Группа www.antiphishing.org). Оповещения включали адреса фишинговых сайтов и связанные имейлы. Этого было достаточно для Макса, чтобы проникать на сервера фишеров и перепохищать украденные данные. После чего он удалял информацию на серверах, чем крайне разочаровывал фишеров.

Другие атаки были менее нацелены, Макс всё еще входил в ряды white-hat хакеров, и присутствовал в адресатах частной e-mail рассылки, где часто раскрывались 0-day уязвимости. Днями и ночами компьютеры Макса сканировали сервера в поисках уязвимостей. Однажды, Макс сканировал Windows сервер на предмет переполнения буфера и нашел то, что привело его в мир кардеров.

Windows сервер, который он сканировал, находился в офисе ресторана Pizza Schmizza в Ванкувере, штат Вашингтон. Он знал это место, это было неподалеку от материнского дома. Изучив содержимое компьютера, он узнал что его использовали как бэкенд для POS терминалов ресторана. С помощью этого компьютера собирались данные по транзакциям с картами, а затем, раз в день, отправлялись в процессинговый центр одним заходом. Макс узнал, что файлы, содержащие

информацию по транзакциям, а также полные данные с магнитной полосы карт, были некриптованы.

Более того, в системе сохранялся бэкап всех файлов с данными по транзакциям, начиная со дня установки систему — уже 3 года. Так Макс скопировал себе данные более чем 50,000 транзакций и удалил оригинал файлов. В конечном счете ресторану эти данные не нужны, да и хранение этих данных противоречило стандартам безопасности Visa. Макс отсортировал данные, убрав дубликаты и дампы просроченных карт.

Впервые у Макса появился основной источник чистых карт, которые практически гарантировано были прибыльными. До сих пор Крис жаловался, что некоторые дампы Макса были устаревшими, больше этого не будет. Когда клиент заказывал большой, семейный пирог в Pizza Schmizza, Макс получал дамп его карты до того как остаток пирога успевал остыть.

Макс закончил очистку полученных дампов и дал Крису протестировать, заметив, что дампы очень свежи, двухдневной давности.

Теперь Крис и его команда никак не могли «переварить» те 50 дампов в день которые Макс получал с Pizza Shmizza. Макс решил предпринять первые шаги в продаже на кардинговой сцене, Крис предложил ему обеспечивать продажи дампов за 50% навара.

Но Макса беспокоила бесшабашность Криса, тот везде скупал золото, оставляя полицию лишь на шаг позади. В тоже время Крис слишком многое знал про Макса и для Макса было сложно ему отказать. Макс дал свое согласие и Крис начал представлять его интересы в подполье.

Скоро Крис заявил Максу о продаже дампов, в то время как Макс, используя бекдор на компьютере Криса знал, что Крис не продает, а сам использует дампы. Для Макса не было никакой разницы в плане навара, однако его терзала мысль, что его обманывают. Это вынудило Макса начать поиски партнера, кого он мог бы с легкостью контролировать.

Со временем, Джон Джианоне, подросток с Лонг Айленда, стал заменой Крису. Джианоне был умным пареньком из семьи среднего сословия, он немного баловался коксом и безумно желал стать жестким киберпанк-оторвой. Делишки, которые провернул Джианоне, откровенно говоря, ничуть не впечатляли, перед кардерами он хвастался, что зажал все кнопки в лифте и следующему зашедшему в лифт пришлось останавливаться на каждом этаже. Еще он хвастался, как в банке, на форменном бланке для заявлений написал «У меня бомба, гоните деньги, либо подорву всех» и поставил в стопку пустых бланков.

В 17 лет Джианоне присоединился к Shadowcrew и CarderPlanet под руководством MarkRich и стал участвовать в маленьких операциях. Его репутация запятналась, когда он попался на подделке авиабилетов, поползли слухи, что он на постоянной основе подворовывал на форуме. Отчаявшись, Джианоне заплатил более успешному кардеру за эксклюзивное право быть под его опекунством. Под ником «Enhance» подросток стал более заметным, но это не сказывалось на его успешности.

В мае 2003, он попытался повторить схему шантажа, придуманную русскими хакерами. Джианоне одолжил у одного хакера ботнет и начав DDoS-ить авиакомпанию JetBlue, положив вебсайт на каких-то двадцать пять минут. Потом он отправил в авиакомпанию имейл с требованием выплатить ему 500,000$ за крышевание в киберпространстве. Однако компания решила не платить, и даже не признала действий кибергангстера, на следующий день компания заявила, что они перешлют имейл в соответствующий правоохранительный отдел и отметили что сайт упал по причине системных апгрейдов.

Макс нашел Джианоне с помощью своей программы Free Amex, парень делал свои дела с компьютера который находился в спальне его матери. Макс и Крис просмотрели данные по Джианоне, и решили, что он годился как партнер. Крис в частности видел в парне самого себя — молодой, балующийся коксом, косящий под гангстера. Джианоне часто бывал в Оранж Каунтри, он любил там понежится на солнышке. Крис тоже начал отдыхать в Оранж Каунтри и завел дружбу с Джианоне, своему подмастерью Крис дал кличку — «Пацан» («the Kid»).

Так получилось, что Макс знал о Джианоне всё, в то время как Джианоне не знал ничего о Максе. С точки зрения Макса это было идеальное условия для сотрудничества. Джианоне продал несколько дампов предоставленных Максом, а затем представил Макса в кругу других кардеров, которые были заинтересованы в покупках используя для связи ICQ. Макс работал под ником «Generous».

Работа с незнакомцами стала большим шагом для Макса, и он предпринял все необходимое для своей безопасности. Для переписки на форуме кардеров он использовал собственную частную сеть взломанных компьютеров, это гарантировало, что как максимум его могли бы отследить до взломанной соседской Wi-fi сети, но это было бы нелегко. Для большей безопасности, Макс сменил свой стиль письма, опасаясь что, кто-либо мог найти совпадение в стиле его сообщений на кардерском форуме с багтреками или постами, оставленными от имени Макс Вижн. ФБР уже обращало внимание на многочисленные, кажущиеся знакомыми, фразы в анонимном письме, которое Макс отправлял в лабораторию Lawrence Berkeley во время BIND атаки.

Прибыль со сделок Макс получал на анонимный e-gold аккаунт, привязанный к

платежной карточке. Пацан зарегистрировал бизнес аккаунт в Bank of America, для регистрации он указал компанию по ремонту автомашин — A&W Auto Clinic, затем выслал Максу дамп магнитной полоски и PIN код. Макс сделал себе дубликат с помощью MSR206, теперь покупатели дампов могли делать наличный вклад на счет A&W Auto Clinic в любом филиале Bank of America и Макс получал деньги на клонированной карточке.

Максу не были нужны деньги, он потратил большинство обналиченных денег после операций с Citibank на подачки бомжам и покупку робопса Sony AIBO за 1500$.

В то же время, Макс был далеко не на нуле, он устроился на хорошо оплачиваемую работу системным администратором в традиционном бизнесе компании Second Life — трехмерного виртуального мира с тысячами посетителями.

Была лишь одна причина, по которой Макс рисковал всё больше и больше — зависимость от стиля жизни профессионального хакера. Макс был без ума от свободы, игр в кошки-мышки, анонимности и огромной власти. Прикрытый анонимностью, находясь в своей безопасной квартире, Макс мог предаваться любым желаниям, исследовать любой потаенной закуток сети и потакать любым своим желаниям без страха за последствия. Макс отвечал только перед своей собственной совестью.

И всё же, где-то в глубине сердца, криминальный хакер оставался мальчишкой. Мальчишкой, который не может устоять от соблазна и пролезает в школу в полночь, чтобы оставить свой след.

Глава 18. «Брифинг»

В конференц-зале неподалёку от Вашингтона настенный монитор показывал два десятка мужских лиц. Некоторые из них хмурились для снимка в камере, другие улыбались для паспортного фото. Пара ребят выглядели как подростки, едва достигшие полового созревания, другие были старше, смотрелись неопрятно и отталкивающе.

Несколько агентов ФБР, в костюмах и галстуках, собравшись вокруг стола, смотрели на лица международного компьютерного подполья. Для одного из них многие вещи внезапно наполнились смыслом.

В свои тридцать пять, Дж Кейт Мударски в течение семи лет работал агентом ФБР. Но в отделе компьютерных преступлений он был всего четыре месяца и ему многому предстояло научиться. Дружелюбный и с хорошим чувством юмора, Муларски хотел стать агентом ФБР с первого курса Вестминстерского колледжа в Пенсильвании, когда к ним в класс пришел для беседы рекрут из бюро. Он оставался в квалификационном листе даже когда ему приходилось работать на более прозаичных должностях, от продавца мебели в Питсбурге до операционного менеджера национальной сети мебельных магазинов, с пятьюдесятью сотрудниками в подчинении в четырёх магазинах.

В 1997, после восьми лет ожидания, он наконец решил что готов для ФБР. После года проверок и шестнадцати недель обучения в академии ФБР в Квантико, он был приведен к присяге в качестве агента в июле 1998.

По одной из традиций бюро, после выпуска новоиспеченные агенты должны были пронумеровать все местные офисы ФБР в порядке предпочтения для трудоустройства. Он поставил своему родному Питсбургу первый номер — это было место, где Муларски вырос, пошел в школу и встретил свою жену. Его шансы попасть туда улетучились в следующем месяце, когда террористы бомбили посольства США в Кении и Танзании. Опытные агенты ФБР были отосланы из Вашингтона для проведения расследований и Муларски был одним из пятнадцати новобранцев, отправленных на вакантные места в столице — городе, который был в его списке под номером тридцать два.

Довольно быстро Муларски перешел от управления мебельными магазинами к работе над некоторыми из самых важных и значимых расследований ФБР. Когда в 1999 передающее устройство было найдено в офисе на верхнем этаже штаб-квартиры Госдепартамента, он был в команде, которая обнаружила российского

дипломата, принимавшего сигнал снаружи. В 2001 он помог выследить Роберта Хансена, агента контрразведки, который в течение двадцати лет занимался шпионажем для КГБ и ФСБ.

Это была головокружительная работа, но секретность раздражала Муларски: его работа была совершенно секретной и он не мог говорить о ней ни с кем — даже с женой. Так что когда штаб-квартира начала искать двух опытных агентов для запуска амбициозной инициативы в области киберпреступлений в Питсбурге, он увидел шанс попасть домой и выйти из тени одновременно. Его новая работа была уже не в офисе ФБР. Он был назначен на должность в офисе некоммерческой организации, называвшейся National Cyber Forensics and Training Alliance. NCFTA была основана банками и интернет-компаниями несколько лет ранее, чтобы отслеживать и анализировать случаи мошенничества против клиентов, по большей части фишинга. Работа Муларски не состояла из разбора отдельных эпизодов, так как каждый из них был слишком мал, что бы превысить по сумме порог ФБР — $100,000. Вместо этого он отслеживал тенденции атак, которые могли бы вывести на виновника — одного или группу хакеров, ответственных за большое количество киберпреступлений. Затем он отправлял результат в местные офисы ФБР и таким образом ему удавалось передать расследование дальше.

Это был лишь сбор информации — нудное, но интересное занятие. Муларски не принимал участия в делах и никогда не получал удовлетворения от надетых на плохого парня наручников. Зато впервые за семь лет он мог поговорить с женой о своей работе за ужином.

Наконец, он вернулся в столицу на свой первый брифинг на тему махинаций с картами. Во главе комнаты стоял почтовый инспектор Грег Крэбб, плотный человек с уставшими глазами, работавший в почтовом офисе международного мошеннического отделения. Крэбб попал в криминальную сферу в 2002 во время отслеживания программного обеспечения для кардинга. С тех пор он побывал в двадцати пяти странах, где, работая с местной полицией, ему удалось собрать большое количество персональных данных членов растущего сообщества хакеров: никнеймы, IP-адреса, переписки и почтовые сообщения более чем двух тысяч человек. Он стал главным экспертом правительства в этой области, но скоро степень его значимости стала угрожать его безопасности. Так он пришел в ФБР за помощью.

Брифинг для полудюжины ФБР агентов проходил в невзрачном Калвертоне, в офисе, где бюро проводило свою операцию по борьбе с детской порнографией. Почтовый инспектор говорил со средне-западным акцентом, не торопясь, будто бы взвешивая каждое слово как посылку, рассказывал историю сцены кардинга: «CardersLibrary» породившая «CarderPlanet», легенда о «King Arthur», влияние

русских и украинцев, взлет и падение «Shadowcrew». Он вытащил скриншот «CarderPlanet», что бы показать структуру подполья: операционный сайт был «доном».

Администраторы — «капо». Это была метафора с использованием интуитивно понятных агентам ФБР терминов: хакеры были новой мафией.

Операция “Firewall”, по словам Крэбба, оставила кардеров в рассеянном, параноидальном и дезорганизованном положении. Но они сумели восстановиться. К тому же теперь, в случае с «Shadowcrew», не было единого объекта для преследования. Вместо этого стало возникать большое количество более мелких новых форумов. Крэбб не сказал этого, но спецслужбы лишь «ввели» кардерам половинную дозу пенициллина: выживших стало больше и они стали «иммунны» к подобным воздействиям.

Муларски ловил каждое слово. За то небольшое время, которое он провел в NCFTA, ему приходилось работать лишь с сырыми данными, всплывающими из подполья: ссылки на никнеймы, зашифрованные сообщения, форумы. Это всё начинало сходиться теперь. Кардеры снова начали самоорганизовываться. Когда Крэбб закончил своё выступление и другие агенты начали собираться, Муларски подошел к инспектору и с энтузиазмом протянул ему руку. «Это был захватывающий материал». Произнёс он. «Я хотел бы работать с вами. Я хотел бы стать вашим партнером.»

Крэбб был очень удивлен такому предложению. По его опыту, куда более типичным для агента ФБР было бы что-то вроде «Давайте мне всю вашу информацию. Спасибо, до свидания». Он встретился с Муларски и его начальником в частном порядке для более тщательного изложения имеющейся информации.

Муларски вернулся в Питсбург, но мысли его блуждали. Он думал, что оставил позади мир русских шпионов, двойных агентов и совершенной секретности. Он ошибался. И его безопасная размеренная новая работа оказалась под большой угрозой.

Глава 19. «Рынок Кардеров»

Как Макс ни старался, он не мог прижиться ни на одном из новых форумов прораставших на руинах Shadowcrew. Все они были коррумпированы, принадлежали продавцам, которые враждебно относились к конкурентам извне. В некотором смысле, это было благословлением. Он никогда не мог полностью доверять любому из этих сайтов — он слишком хорошо понимал, что эта сцена полна полицейских и информаторов.

Наконец он пришел к выводу: если бы он и стал торговать, единственной площадкой мог стать только сайт, которым владеет он сам. Все еще воображая себя Робин Гудом, он выбрал идеальное имя для своего форума: Шервудский лес (Sherwood Forest).

Крис согласился с этим планом — ему нравилась идея продавать поддельные кредитные карты и водительские удостоверения в безопасной среде — но его бесило название. С точки зрения брендинга, «Шервудский лес» не особо подходило для криминального рынка. Партнеры снова вернулись к вариантам, и в июне 2005 Макс, используя вымышленное имя и фиктивный адрес в Анайхеме, зарегистрировал Cardersmarket.com.

Это был критичный для Макса период: подходил к концу срок федерального надзора за ним, как за условно-досрочно освобожденным, и, если бы он продержался до полуночи 10 октября 2005 года, он был бы свободным человеком не обязанным играть роль частичного занятого компьютерного консультанта перед своим куратором по досрочному освобождению. Это должно было быть достаточно просто — выдержать еще несколько месяцев. Кроме самого Криса, о двойной жизни Макса знали оба друга Криса: Джеф Нормингтон и Вернер Дженер, мошенник в сфере недвижимости выписавший Чарити чек на 5 000 долларов, который помог Максу вернуться к хакерству.

Позже, в сентябре 2005, Вернера арестовали.

С самого начала их взаимоотношений с Максом, Крис подкидывал Дженеру небольшое количество карт от случая к случаю — может быть около 80 за более чем 3 года — в обмен на 10 процентов от покупок Дженера. В этом месяце Дженер попросил две дюжины карт — финансовые проблемы вынудили его продать свой семейный дом в Лос-Анджелесе и он переехал в Вестпорт, штат Коннектикут, чтобы начать все заново. Вскоре после этого, сообщник по криминальным делам ограбил его — Дженер потерял практически на весь доход с продажи дома, и ему

требовалось увеличить доходы, чтобы содержать себя и свою жену с тремя детьми.

Когда посылка Криса пришла, Дженер — страстный коллекционер часов, отправился прямиком в Richards — магазин мужской одежды и аксессуаров в Гринвиче, где продавались топовые модели хронометров. У Дженера был качественный «пластик» и удостоверение личности на имя Стивена Лихи. Чего у него не было, так это опыта в кардинге. Он выбрал не одни, не двое, а четверо часов Anonimo стоимостью от 1 до 3 тысяч долларов каждые. При этом попросил владельца магазина пробить все часы отдельно и оплатил их четырьмя разными картами Visa, которые открыто вытягивал из целой пачки карт. Две весьма больших транзакции были отклонены и в результате Дженер получил только двое часов общей стоимостью в 5 777 долларов, оплаченных картами Bank of America.

Патрульная машина нагнала его через пару миль. Пока полицейские проверяли настоящее водительское удостоверение Дженера и уточняли не покупал ли он только что часы, вторая машина подъехала с владельцем магазина, который подтвердил, что они остановили того самого парня.

Полицейские арестовали Дженера и обыскали его машину, найдя часы, 28 кредитных карт, 6 водительских удостоверений на разные имена. Когда детективы получили ордер на обыск его дома, они нашли еще несколько часов и пистолет Walter P22 двадцать второго калибра.

Пистолет знаменовал плохие новости. Вместо обвинения в воровстве и нарушении правил условного освобождения, Дженера теперь ждало обвинение в незаконном хранении огнестрельного оружия. Не теряя времени, он предложил привести федералов к источнику поддельных карт. В соответствии со стандартными условиями для стукачей, правительство согласилось принять эту информацию в обмен на ограниченный иммунитет: ничего из сказанного Дженером не будет использовано против него. Если информация окажется полезной — приведет к арестам — они рассмотрят возможность рекомендовать сократить срок по обвинению в хранении оружия.

За два совещания суммарной длительностью в 8 часов Дженер выложил все, что знал, местным агентам Секретной Службы и федеральному прокурору. Он рассказал им о Крисе Арагоне — его цепочке обнальщиков, и «Хакере Максе» — двухметровом компьютерном гении, который взламывал банки из отельных номеров в Сан-Франциско.

Он не знал фамилию Макса, но вспомнил, что однажды выписал чек на 5 000 долларов подружке хакера. Ее имя было Чарити Мейжерс.

Секретная Служба запротоколировала интервью и внесла информацию в

компьютер агентства, но агентство так и не проверило эти данные, поэтому прокуроры отказали Дженеру в особых условиях рассмотрения его дела. Он был приговорен к 27 месяцам тюрьмы.

Макс Вижн увернулся от пули. Показания Дженера утонули в гигантском правительственном компьютере — с таким же успехом их можно было спрятать в пещере из финальной сцены фильма «В поисках утраченного ковчега». До тех пор, пока ни у кого не было повода их раскапывать, Макс был в безопасности.

Тем временем, Макс начал процесс становления Cardersmarket. У него было немало опыта в запуске легальных сайтов, но криминальный сайт требовал особой подготовки. К примеру, что он не мог разместить сервер Cardersmarket прямо на полу своего дома — это сделало бы его легкой мишенью.

Он взломал работающий через провайдера Affinity Internet дата центр во Флориде и установил виртуальную машину VMware на один из их серверов, спрятав целый компьютер в их системе. Его спрятанный сервер присвоил один из неиспользованных адресов Affinity. Сайт станет кораблем-призраком, никому не принадлежащим и никем не обслуживаемым.

Макс поиграл с различными интернет-форумами и наконец остановился на гибком движке vBulletin. Он потратил месяцы на настройку внешнего вида и дизайн шаблонов для внешнего вида сайта, стилизуя его в оттенках серого и приглушенного золотого цвета. Работа выглядела удовлетворительно. Впервые за несколько лет он создавал что-то, а не воровал. Это было так же, как разработка Whitehats.com, кроме тех моментов, которые находились по другую сторону.

Наконец, на первую годовщину операции «Firewall», он внес новое имя в свой постоянно меняющийся список псевдонимов: Iceman. Одной из причин выбора такого прозвища стала его обыденность: в подполье было полно Iceman‘ов, даже на Shadowcrew был один. Если бы правоохранительные органы попытались его отследить, они бы видели несколько миражей на своем радаре.

Под скромные фанфары, Iceman запустил Cardersmarket.com в конце 2005 года. Крис присоединился в качестве первого со-администратора, взяв себе ник EasyLivin.

После осторожных наблюдений за Shadowcrew и мелкими форумами-последователями, Макс и Крис понимали, что ключом к получению признания будет назначение на управляющие позиции известных людей, которые помогали бы поддерживать форум и привлечь еще больше тяжелой артиллерии из своих друзей. Скоро партнерам удалось привлечь двоих известных людей из диаспоры Shadowcrew.

Бредли Андерсон, 41-летний выпускник Цинциннати, был их первым приобретением. Андерсон был легендой под ником «ncXVI» — эксперт по поддельным удостоверениям личности, автор самостоятельно изданной книги Сбрасывая кожу (Shedding Skin) — библии по изменению личности.

Вторым рекрутом был Бретт Шеннон-Джонсон 35-ти лет из Чарльстона, штат Южная Каролина, похититель персональных данных известный в онлайне, как «Gollumfun» — основатель Библиотеки фальшивок и Shadowcrew отошедший от дел во времена второго сайта до того, как секретная служба уничтожила его.

После того, как он пропал со сцены более, чем на год, Джонсон пытался вернуться в дело. Подельник Криса Джон Джианноне заметил его онлайн весной и завел диалог по ICQ, вводя его в курс дела по последним арестам и сплетням.

Джианноне раззадорил Джонсона продав ему 29 дампов Макса всего за 600 баксов, потом представил его Максу, который продал ему еще 500 карт. «Я вижу, что мы с тобой будем делать хороший бизнес в будущем», — сказал Максу Джонсон.

Джонсон принял предложение Макса и Криса стать админом на Carders Market, обеспечивая сайт опытом и контактами единственного администратора Shadowcrew пережившего операцию «Firewall».

Джианноне присоединился к Carders Market под ником «Zebra», а Макс создал себе второй аккаунт с псевдонимом «Digits». Альтернативная личность была ключевой особенностью в новой бизнес-стратегии Макса. Shadowcrew пал, потому что прокуроры доказали, что основатели сами покупали, продавали и использовали краденные данные, а управление информационным веб-сайтом само по себе не являлось нелегальным, сделал заключение Макс. Итак, Iceman должен быть лицом Carders Market, но никогда не будет покупать или продавать ворованные данные. Digits — его альтер эго — займется этим, продавая дампы, которые Макс получал из Ванкуверской пиццерии, любому, кто может их приобрести.

Чтобы завершить свое видение сайта, Максу был нужен еще один админ с определенными навыками: владеющий русским языком. Он хотел восстановить пропасть, которую проделала операция «Firewall» между Восточной Европой и их западными коллегами. Двое русских участников Shadowcrew попались в VPN-ловушку Cumbajohnny, и вся эта ситуация заставила русских относится к англо-говорящим форумам с огромным подозрением.

Макс решил, что Carders Market выделится за счет Восточно-Европейской секции модерируемой коренным русским. Ему оставалось только найти кандидата.

Крис предложил помочь и Макс согласился. Если и была какая-то вещь, которую Крис доказал своему партнеру, так это то, что он знал как привлечь новые таланты.

Глава 20. «Starlight Room»

С потолка, прямо над роскошными диванами клуба «Starlight Room», владельцем которого был Гарри Дентон, свисали девять винтажных люстр, лучи стокилограммового зеркального шара бегали по поверхности танцплощадки. Огромные тёмно-красные шторы свисали по обе стороны широких панорамных окон, словно сценические занавеси, за которыми было видно огни небоскрёбов Сан-Франциско.

Расположенный на двадцать первом этаже отеля «Sir Francis Drake», клуб «Starlight Room» был одним из самых дорогих ночных клубов этого города и неотъемлемой частью его бурной ночной жизни с интерьером в стиле 1930-х годов, отделанным тёмно-красной дамастовой тканью и шёлком ручной выделки. Скорее кричащему, чем стильному клубу удавалось привлекать клиентов только благодаря регулярным тематическим вечерам. В ту среду клуб организовывал «Русскую вечеринку», поэтому кругом гремела музыка с Родины, а официанты в смокингах разливали водку столпившимся возле стойки бара посетителям.

В женском туалете кто-то целовал Тсенгельтсетсег Тсетсендельгер. Уже успев выпить в тот вечер, молодая монгольская иммигрантка не помнила, как так случилось, или зачем, что длинноногая брюнетка захотела её поцеловать. Спустя мгновение глаза Тсенгельтсетсег округлились от удивления. Рядом стояла ещё одна брюнетка, точная копия первой.

Мишель и Лиз представились, и на лице Тсенгельтсетсег появилась широкая, непритворная улыбка. Она сказала близняшкам Эскере, что они могут звать её просто «Ти», по первой букве её фамилии.

Ти регулярно посещала русские вечеринки в этом клубе и без проблем изъяснялась на русском и английском. Родом из северной части Монголии, она ещё застала времена, когда страна находилась под влиянием Советского Союза. Русский она учила в школе до тех пор, пока Советская империя не распалась и монгольский премьер-министр не объявил английский язык вторым официальным языком.

Предвкушая большое приключение и пресловутую «лучшую жизнь», в 2001 году она смогла получить студенческую визу и эмигрировать в США. Её первой мыслью после прибытия в лос-анджелесский международный аэропорт было то, что американцы действительно ужасно толстые. Но позже, попав в город, её впечатление изменилось в лучшую сторону: Лос-Анджелес был полон замечательных людей.

Проучившись один семестр в двухгодичном колледже в Торрансе, она переехала в Сан-Франциско, где получила грин-карту. Теперь она училась в колледже Перальта в Окленде и подрабатывала продавщицей мороженого в кафе «Fenton's Creamery», благодаря чему могла оплачивать квартиру и учёбу.

Лиз как-то особенно заинтересовал тот факт, что Ти знала русский. Близняшки принесли Ти напиток из бара, после чего предложили продолжить вечеринку вместе с их друзьями в гостинице неподалёку. Было уже за полночь, когда они пришли в номер их друга, Криса Арагона, в отеле «Clift» возле площади Юнион-сквер. Крис, отдыхавший там с друзьями, сразу же очаровал Ти своей внешностью. Он, казалось, тоже проявил к Ти интерес, который усилился, когда близняшки упомянули, что она знала русский. В компании ещё двух сотрудниц Криса они открыли несколько бутылок с алкоголем и гуляли до раннего утра. Когда остальные девушки разошлись по своим комнатам, Ти осталась ночевать в комнате Криса.

Следующим утром, когда Ти ещё досматривала свой последний сон, в комнате началось активное движение. Лиз и несколько других симпатичных девушек — все оживлённые и вычищенные, без следа ночных гуляний — поочерёдно забегали в комнату и выбегали из неё с конвертами и зашифрованными посланиями от Криса.

Весь день продолжался в том же духе: девушки забирали конверты, приносили сумки, иногда оставались ненадолго в номере, затем уходили снова. В воздухе чувствовалась праздная атмосфера предыдущего вечера, но к ней добавилась нотка нервозности или возбуждённости, приводившая Ти в недоумение — но не настолько сильное, чтобы она начала задавать вопросы.

Вечером, уже когда стемнело и компания собралась в номере, Ти сказала, что уходит. Ей нужно было возвращаться домой в Ист-Бей, чтобы быть вовремя на работе в кафе следующим утром.

Крис предложил ей кое-что получше. Он недавно запустил веб-сайт с одним своим коллегой по бизнесу, «Сэмом», и как раз им нужен был русский переводчик на полную занятость. Она бы зарабатывала больше, чем ей платят в кафе за скармливание шоколадного мороженого с орешками молодым бизнесменам.

— Не уходи, — сказала Лиз. — Ты с нами больше будешь зарабатывать.

Ти посмотрела на своих вновь приобретённых друзей. Они ей напоминали новых русских, которые после крушения советского режима набивали свои кошельки деньгами, приобретёнными сомнительными путями, и пожирали все и вся с большой жадностью и малым чувством вкуса.

Но Крис ей нравился; он ей казался другим. К тому же, делая переводы для веб-

сайта, у неё была бы свобода и гибкое расписание, она могла бы сконцентрироваться на учёбе. Ти согласилась.

На следующий день Крис скомандовал своей команде собираться и объявил, что их следующим пунктом назначения будет Лас-Вегас. Он сказал Ти встретить их уже там, будет весело. Ей следовало завести электронную почту на Yahoo. Она собрала сумку и отправилась в аэропорт.

Крис помог Ти переехать поближе в район, где он сам жил, и заплатил за аренду квартиры в Дана-Пойнт, прибрежном городке в округе Ориндж, которую он снял на её настоящее имя. Стоящий в конце тихого, петляющего переулка, покрашенный в оранжевый цвет итальянских домиков и с крышей из испанской черепицы, «Чайный домик», как он его окрестил, был словно другим миром, по сравнению с Монголией, где выросла Ти.

Они занялись любовью на её новой кровати, после чего Крис оставил 40 долларов на ночном столике, чтобы она сходила в маникюрный салон. Ти обиделась на это. Она не какая-нибудь проститутка. Она полюбила его.

Крис и его команда перевезли своё оборудование для изготовления карточек с Вилла-Сиена в гараж квартиры в Дана-Пойнт — «Чайный домик» теперь будет его новой базой, местом для вечеринок и местом круглосуточной работы Ти в «Carders Market». Её обязанности: находить онлайн-форумы энтузиастов из восточно-европейских стран, занимающихся подделыванием платёжных карточек, такие, как «Mazafaka» и «Cardingworld», и резюмировать происходящее там для использования в русской секции «Carders Market».

Ей понадобится ник, объяснил Крис, имя или прозвище для её альтер эго в онлайн-мире. Она выбрала ник «Alenka», название известной русской шоколадки.

Alenka сразу же ринулась в работу, день и ночь сидя перед монитором компьютера, искренне пытаясь разыскать влиятельных русских и переманить их на веб-сайт Криса и «Сэма», также известного как «the Whiz».

Глава 21. «Мастер Сплинтр»

Занимая целый этаж зеленого офисного строения на берегу реки Мононгахила, Национальный Альянс Кибер-Криминалистики и Обучения (НАККО) был весьма далек от секретности Вашингтонского разведывательного сообщества, где Муларски делал первые шаги. Здесь дюжины экспертов по безопасности из банков и технологических компаний работали наряду со студентами из близлежащего университета Карнеги-Меллон в кучно расставленных аккуратных кабинках, окруженных кольцом кабинетов и, затем, стенами здания из тонированного стекла. Со стульями Aeron и вайтбордами, офис создавал ощущение одной из технологических компаний, которые снабжали НАККО основной частью средств. ФБР внесли несколько изменений перед тем как въехать, переделали один из кабинетов в комнату с электронными коммуникациями, заполнили ее компьютерами одобренными правительством и шифровальным оборудованием, чтобы безопасно коммуницировать с Вашингтоном.

В своем кабинете Муларски изучил схему связей Крэбба — почтового инспектора, который прислал ее по e-mail — большая схема показывающая различные связи между 125-ю целями из подполья. Муларски осознал, что он делал все неправильно: ожидал преступления, а потом пытался вычислить виновников. Преступники вовсе не прятались. Они рекламировали свои услуги на форумах. Это делало их уязвимыми, так же, как ритуалы и строгая иерархия Нью-Йоркской и Чикагской мафии, которые дали ФБР инструкцию чтобы сломить банды десятилетия назад.

Все что ему надо было сейчас сделать — это присоединиться к кардерам.

Он выбрал форум из списка, который прислал ему Крэбб и нажал на ссылку регистрации аккаунта. Согласно правилам Департамента Юстиции, Муларски не мог внедряться на форумы без согласования с Вашингтоном, условия которого предполагали, что он будет соблюдать строгие ограничения в своей деятельности. Чтобы сохранять свое прикрытие, он мог размещать сообщения на форумах, но он не мог взаимодействовать с кем-то напрямую; ему будет разрешено не более, чем три «существенных контакта» с любыми из участников форума. Участие в преступлениях или совершение контрольных закупок было за границами дозволенного.

Все это могло быть только операцией по сбору данных; он будет губкой впитывающей информацию о своих противниках.

Как только он зарегистрировался, перед ним встала необходимость принять первое важное стратегическое решение: каким будет его ник. Муларски доверился своей интуиции. Вдохновленный мультфильмом «Черепашки-ниндзя», который показывали по утрам, агент остановился на кличке грызуна-сенсея живущих в канализации мастеров карате — двуногой крысе по имени Мастер Сплинтер. Для уникальности и придания хакерской нотки, он писал его фамилию без «лишних» гласных. (Splinter — Splyntr).

Итак, в июле 2005 Мастер Сплинтр зарегистрировался на своем первом криминальном форуме CarderPortal, смеясь про себя над игрой смыслов — для подпольного форума он взял имя подпольной крысы.

Вскоре Муларски играл на кардерских форумах, как на шахматной доске, опираясь на поток данных НАККО о мошенничествах для своих ходов.

Центр был включен напрямую в противодействие мошенничеству, связанному с банками и сайтами электронной коммерции, так что когда появлялась новая криминальная инновация, Муларски знал о ней. Он постил их схемы на CarderPortal, выдавая за собственные изобретения.

Продвинутые мошенники давались диву с новичка, который самостоятельно осваивал все их новейшие фишки. Когда способы мошенничеств становились доступны для широкой публики и появлялись в СМИ, новички помнили, что впервые услышали их от Мастера Сплинтра.

Тем временем, агент ФБР впитывал историю форумов, оттачивая свой словарный запас, чтобы соответствовать циничному, нецензурному стилю подполья.

Через несколько месяцев Муларски столкнулся с первым вызовом в его операции по сбору сведений. Первые форумы выросшие на развалинах Shadowcrew принимали новых членов с распростертыми объятиями — напуганные операцией Фаервол, многие мошенники взяли новые прозвища и, в отсутствии репутации, при торговле кардеры не имели никакой возможности проверить друг друга. Теперь эта ситуация менялась. Возник новый вид «поручительских» форумов. Единственным способом попасть туда было получение поддержки двух действующих участников. Но ведь Муларски связанный ограничениями Департамента Юстиций намеренно избегал выстраивания прямых связей с подпольем. Кто поручится за него?

Заимствуя идею из романа Роберта Ладлэма, Муларски решил, что Мастер Сплинтр нуждается в легенде, которая сможет продвинуть его на новые криминальные форумы. Его мысли были направлены в сторону европейской организации по борьбе со спамом под называнием «Spamhaus» с которой он работал в рамках предыдущих операций ФБР.

В основанной бывшим музыкантом в 1998 году Spamhaus, составляли списки постоянно меняющихся интернет-адресов распространявших мусор по почтовым ящикам потребителей; их базу данных источников спама использовали две трети международных интернет-провайдеров в качестве черных списков. Более интересным для Муларски был составляемый этой же компанией список самых разыскиваемых спаммеров.

Состоящий из таких, как Алан «Spam King» Ральски и русский Лео «BadCow» Куваев, Реестр Известных Спам-Операторов (англ. аббр. — ROKSO), уступал только федеральным обвинительным актам в части списков, в которых мошенники не хотели бы обнаружить свое имя.

Муларски позвонил основателю Стиву Линфорду в Монако, чтобы объяснить схему: он хотел попасть в ROKSO или, по крайней мере, чтобы Мастер Сплинтр туда попал. Линфорд согласился и Муларски продолжил работать над своей легендой. Лучшая ложь всегда основана на правде, так что Муларски решил сделать Сплинтра польским спаммером. Муларски по отцу был из польских иммигрантов — выданная бюро рубашка скрывала татуировку Orzel Bialy (польск. — Белый Орел) на его левой руке — белый орел с золотым клювом и когтями, который украшал польский герб. Муларски расположил Мастера Сплинтра в Варшаве, он бывал в польской столице и мог при необходимости достаточно сносно описать достопримечательности.

В августе списки ROKSO вышли в свет впервые связывая «настоящее» имя с придуманным Муларски мультяшным альтер-это.

> Павел Камински aka «Мастер Сплинтр» управляет слабо организованной командой спаммеров и мошенников из Восточной Европы. Возможно партнер BadCow. Он связан со спамом через прокси, фишингом, pump‘n‘dump, эксплоитами, форумами кардеров и ботнетами.

Профиль содержал примеры мошеннических спам-сообщений предположительно отправленных «Павлом Камински», созданных в Spamhaus, и анализ расположения его хостингов.

Теперь кардеры, которые загуглят Мастера Сплинтра могли убедиться, что он был настоящим, добросовестным хакером замешанным во многих скользких делах. Когда Муларски зашел на CarderPortal, он увидел во входящих сообщениях несколько бизнес предложений от мошенников, надеющихся сотрудничать с ним. Все еще ограниченный запретом впрямую взаимодействовать с подозреваемыми, он

презрительно отшивал их.

Ты не очень-то большой игрок — отвечал он. Я не хочу с тобой работать, потому что я профессионал, а ты, очевидно, новичок в этом. Чтобы отшить мошенников высшего эшелона, он бросал вызов их кошельку: у тебя недостаточно денег, чтобы вложить в то, чем я занимаюсь.

Как недоступность девчонки на выпускном, отчужденность Мастера Сплинтра лишь делала его еще более привлекательным. Когда запустился новый закрытый форум под названием Международная Ассоциация Развития Преступной Деятельности (англ. аббр. — IAACA), он разместил простой пост: «Привет, мне нужно поручительство», — и двое существующих членов поручились исключительно за его репутацию.

Затем он получил поручительство для Theft Services, потом для CardersArmy. В ноябре 2005-го он был одним из первых, кого пригласили на новый форум Darkmarket.ws.

Несколько месяцев спустя, другой, конкурирующий сайт вырос достаточно, чтобы попасть на его радар. И Мастер Сплинтр присоединился к Cardersmarket.com.

Глава 22. «Враги»

Джонатан Джанноне выучил, что потеря личной жизни это цена за работу с Iceman.

Он работал с таинственным хакером в течение года, в основном приобретая серверы, которые Iceman использовал для сканирования уязвимостей, но все равно был под постоянным электронным королем со стороны Iceman. Однажды, хакер отправил Джанноне ссылку на новость якобы на сайте CNN о компьютерной проблеме в JetBlue, авиакомпании, которая дала отпор вымогательствам Джанноне давным-давно. Джанноне не думая кликнул по ссылке и тогда Iceman опять попал в его компьютер. Сработала атака типа Client-side.

Джанноне начал регулярно проверять свой компьютер на наличие вредоносных программ, но все равно не мог отслеживать все вторжения Iceman'а. Макс получил пароль Джанноне от премиальной системы United Airlines и начал отслеживать его перемещения по миру. Джанноне был любителем авиапутешествий, который мог запросто отправиться в полет, только для того, чтобы заработать бонусные мили. Когда он приземлился в международном аэропорту Сан-Франциско, в его мобильном уже находилось текстовое сообщение от Iceman'а. «Почему ты в Сан-Франциско?»

Это могло бы показаться забавным, если бы не пугающие перепады настроения Iceman'а. Он мог измениться за секунду — в один день ты будешь для него лучшим другом, в другой он будет уверен, что ты стукач, предатель или еще хуже. Он писал Джанноне длинные спонтанные письма, с жалобами на Криса или других членов сообщества кардеров.

Джанноне понял, это была зависть. Пока он и Крис развлекались в Вегасе и в округе Орандж, Iceman был заперт в квартире, работая как собака. На самом деле, вспышки гнева у хакера часто совпадали с поездками Джанноне в Калифорнию. В июне 2005, Iceman затеял ссору с Джанноне, после его посадки на ранний рейс в округ Орандж, Айсмен хотел привлечь его к ответу, за какую-то оплошность в их совместной операции. Первое сообщение упало на BlackBerry Джанноне в 6 утра, в Сан-Франциско было 3 ночи, и после сообщения сыпались нон-стоп в течение 2500 миль, пока Iceman окончательно не замолчал, после приземления самолета. Когда Джианноне позже проверил свою почту, он нашел десятки писем от извиняющегося хакера. «Прости, я извиняюсь. Я вспылил».

До этого был случай в Сентябре 2004, Джианноне сообщил Iceman'у о своем

плане слетать и встретиться с Крисом, на что Макс мрачно заметил, что он мог бы помешать этой поездке, если бы захотел. Джианноне посмеялся. Однако после 1.5 часа полета его самолет неожиданное развернулся и вернулся в Чикаго. После посадки самолета в международном аэропорту О'Хара, капитан сообщил, что центр управления воздушным движением в Лос Анджелесе пропал, из-за чего пришлось изменить в маршрут.

Оказалось это произошло из-за простой ошибки в компьютере. Это был известный баг в системе радио-управления, базированной на операционной системе Windows, центра управления воздушным движением города Лос Анджелес в Палмдейл, который требовал технической перезагрузки каждые 49.7 дней. Они пропустили момент перезагрузки, а резервная система штатно не запустилась. В результате отключения сотни самолетов были посажены, а так же было зафиксировано пять инцидентов нахождении самолетов на расстояние ближе, чем разрешали правила безопасности. Не было обнаружено злого умысла, но спустя несколько лет, когда были раскрыты все возможности Макса, Джианноне поймал себя на мысли, что Iceman не взламывал компьютеры федерального управления авиации и не выводил из строя Лос-Анджелес, просто чтобы не допустить его встречи с Крисом.

Джанноне, наконец, принял радикальные меры, чтобы попытаться сохранить свои вещи от Iceman. Он купил компьютер от Apple. Iceman мог проникнуть куда угодно, но Джианноне был уверен, что он не сможет взломать Mac.

Пока Макс продолжал следить за его криминальными партнерами, Cardersmarket начал заполняться слухами, усиленными таинственным хвастовством его основателей. Как Iceman и Easylivin, Макс и Крис были неизвестными среди своих собратьев мошенников, однако опытные кардеры могли чувствовать уверенность и уличную смекалку в их сообщениях.

В Сиэтле, имя новому сайту дал Дейв «El Mariachi» Томас, бывший агент ФБР, который, как и Макс, пытался дать отмашку операции Firewall. Томас дрейфовал, с тех пор как федералы отключили его от сбора разведывательной информации, и искал новое в сети из дома.

Опасаясь, Томас зарегистрирован под фальшивым никнеймом. Но когда Iceman пригласил на общественное обсуждение философии и устава «Рынка Кардеров», Томас начал подробно высказываться о направлении, которому должен следовать сайт, чтобы выполнять успешные операции, избегая участи ShadowCrew.

Вначале Крис и Макс подумали, что Томас может быть ценным помощником. Но вскоре они обнаружили, что он был заодно с одним из их выбранных

администраторов, Бреттем «Gollumfun» Джонсоном.

Слухи крутились вокруг Джонсона с тех пор, как он вернулся на сцену. Вы не можете просто пропасть на два года, а после вернуться на форум кардеров как ни в чём не бывало. В августе, хакер «Manus Dei» подлил масла в огонь, взломав почту Джонсона и опубликовал информацию о кардере в группу под названием FEDwatch. Автор публикации сообщил настоящее имя Джонсона, его адрес проживания в Огайо, а так же большое количество персональной информации из его почтового ящика. Среди главных откровений: Джонсон вел переписку с репортером из New York Times о сцене кардеров и владел загадочным доменным именем, Anglerphish.com — возможно домен был подготовлен для собственного сайта.

Там не было ничего, чтобы предположить, что Джонсон был предателем, однако, что Макс, что Крис были встревожены этой информацией. С другой стороны Томас убедил основателя ShadowCrew, что тот был осведомителем. В конце концов, Джонсон сообщил о своей отставке до операции Firewall и потом вернулся без объяснений.

В последнюю очередь Крису и Максу для развития сайта нужна была война между двумя матерыми кардерами из-за разногласий времен ShadowCrew. Тем не менее, одержимый предпринимательской гордостью, Крис хотел сайт, который станет лучшим преступным форумом. Поэтому он обратился к Томасу по ICQ, чтобы попытаться разобраться со всеми проблемами.

«Я не буду разыгрывать драму о Gollumfun, или других, кто крыса, кто не крыса» — писал Крис. «Я просто хочу чистый хороший сайт, чтобы у нас было безопасное место для игры».

Крис пообещал отправить такое же сообщение Джонсону. Он следовал советам из серии «Как договариваться со сложными людьми». Он последовал отеческому совету, попросив Томаса о совете как запустить успешный форум, таким образом, показывая своё уважение более опытному кардеру. Но, чтобы убедиться, что его наставление было воспринято всерьез, Крис предупредил его. «Мы не дети чувак» написал он. «Мы старой закалки. И мы хороши в том, чем занимаемся».

Томас пообещал вести себя хорошо, и добавил, что сделает все возможное, чтобы помочь сделать Cardersmarket форумом без драматичных сцен, как этого желают все. Но в тайне, внутри него созревал комок подозрения. Почему кто-то будет защищать Бретта Джонсона, который явно был стукачом?

Он заметил, что Easylivin’ использовал старую версию ICQ, которая показывала IP адрес. Томас попытался проследить адрес, и он привел его в Бостон, известный рассадник федеральных информаторов. Хостинг «Рынка Кардеров» располагался в

Форт-Лодердейл, штате Флорида, еще одно идеальное место для запуска секретной операции. Номер телефона указанный в контактной информации домена указывал на полицейский департамент Калифорнии, хотя и с другим кодом. Скорее всего, это было совпадение, но кто знает?

Когда он закончил складывать доказательства, у него в животе возникло неприятное чувство. Cardersmarket был подставой федералов. Теперь это было очевидно. Он дал себе слово, что сделает все возможное, что бы уничтожить новый сайт и опустить говнюков «старой закалки» Easylivin'а и Iceman'а.

Глава 23. «Рыба-Удильщик»

Макс занимался сбором информации на Бретта Джонсона. Он начал с проверки логов доступа и личных сообщений админа CardersMarket. Для того, чтобы проверить себя, Макс взломал аккаунт Джонсона на сайте «Международной ассоциации развития преступной деятельности» («The International Association for the Advancement of Criminal Activity», IAACA) и поискал следы его активности. Однако, ни дымящихся пистолетов, ни прочих улик не было.

Неужели он мог привести информатора в узкий круг его нового сайта?

Проблема в том, что нет никакого конкретного метода, чтобы определить, работает ли Джонсон, или кто-то еще на правительство. Макс хотел использовать дыру в безопасности юриспруденции, как переполнение буфера в BIND, которую он мог использовать снова и снова в отношении любого, кого подозревал.

```
If (is_snitch(Gollumfun)) ban(Gollumfun);
```

Он доверился Дэвиду Томасу, не представляя, что Томас уже занес Iceman‘а в свой километровый список врагов.

> Как-то при его проверке, он отправил нам некоторые данные PayPal, которые были верны, но их я пометил как незаконные. Я подумал, окей, этот парень не федерал и не на побегушках у них.
>
> Это было очень важно для меня, потому что от этого зависело, буду я ему доверять, или нет. Мы взяли это на заметку и решили связаться с адвокатом, чтобы он дал нам окончательный ответ, мой товарищ сказал, что займется этим. Хотя я сомневался в том, что мы получим конкретный ответ, потому что адвокатам нравится получать деньги за разного рода предположения, нежели за конкретные факты. Может быть мне попадались плохие адвокаты.
>
> Мне бы очень хотелось знать, смогу ли я найти что-то, что не смогут найти копы или стукач. Что-то, что заставит их планы провалиться на 100%, если они сделают это. Что за Чаша Грааля. Все это время я живу с расчетом, что моя деятельность выдаст их. Как человек, который курит косяк с кем-то, чтобы удостовериться, что он не коп. Или как

> проститутка, которая спрашивает своего клиента: «Вы коп? Если вы коп - вы должны сказать мне об этом.»

Конечно же Бретт Джонсон был по уши в грязи. Однако, вопреки подозрениям, его возвращение к криминалу в пост-фаервольную эру началось не со стукачества. Всё это началось с девушки.

Преступления Джонсона и его кокаиновые привычки за девять лет изгнали его жену. По пути к двери она разбила его MSR206, так что ему пришлось искать психолога, чтобы справиться с потерей. Затем Джонсон встретил Элизабет в баре Северная Каролина. Она была 24 летней танцовщицей в местном стрип-баре, а для Джонсона стала любовью с первого взгляда. Он прожигал свои сбережения, одаривая ее подарками: кошелек за 1500 долларов, пара новых туфель за 600 долларов. Через пять месяцев она переехала к нему. Тем не менее, когда они занялись любовью в свой первый раз, Элизабет не разрешила ему поцеловать себя.

Темные догадки Джонсона подтвердились, когда он нашел Элизабет на сайте, где мужчины делились отзывами о стриптизершах и проститутках. Строчку за строчкой он читал о том, как его подружка оказывает услуги в обмен на деньги и кокаин. Джонсон предъявил ей найденное, на что она, со слезами на глазах, обещала завязать с наркотиками и проституцией.

Надеясь вытащить Элизабет из ее привычного старого образа жизни, Джонсон стал осыпать ее еще более дорогими подарками и водить в дорогие рестораны. Это было реальной причиной его возвращения, ему очень нужны были деньги. Удача, которая выбрала его во время операции «Firewall», отвернулась от него восьмого февраля 2005 года, когда полиция Чарльстона, в Северной Каролине, арестовала его за использование фальшивых чеков Банка Америки при покупке Кругеррандов (золотые монеты в Южной Африке) и часов, выигранных на eBay, которые ожидали оплаты наложенным платежом на его хате. После недели пребывания в окружном центре заключения Чарльстона, тоскуя по Элизабет, Джонсон выбил свидание. После того, как он убедил их, что он был Gollumfun‘ом, - админом, который сбежал, когда копы накрыли ShadowCrew, - они согласились помочь ему, если он будет работать на них.

Секретная Служба снизила залог за Джонсона до 10000 долларов. Когда его освободили, агенты перевезли его из Чарльстона в Колумбию, Южная Каролина, где арендовали ему жилье и платили 50 долларов в сутки. Теперь он был ежедневным посетителем полевого офиса в Колумбии, отмечаясь в 4 вечера и работая до девяти, посвящая Секретную Службу в глубины CardersMarket и прочих форумов. Все, что происходило на мониторе Джонсона, дублировалось на 42-х

дюймовой плазме, что висела на стене офиса. Они назвали это операция «Рыба-Удильщик», и Джонсон думал, что однажды из этого получится классная книга. Вот почему он зарегистрировал домен Anglerphish.com и начал переговоры с журналистом Нью-Йорк Таймс. Когда Манус Дей взломал его ящик и предоставил данные о его активности онлайн, агенты Секретной Службы разгневались. Они отреагировали оперативно, закрыв ему доступ к компьютерам вне офиса и приказав разорвать контакт с журналистом. Элизабет бросила его - ее имя и род занятий были выставлены как нарушение.

Затем Iceman лишил его привилегированного положения на CardersMarket, а мошенники, которых он знал со времен Библиотека фальшивок, стали отказываться от дел с ним. Джонсон выходил из доверия, а у Секретной Службы заканчивалось терпение.

В конце марта 2006 года агенты решили действовать, используя лишь один из уловов операции - мошенника из Калифорнии, который украл, по крайней мере, 200 000 долларов посредством махинаций с налоговыми декларациями. Джонсон как специалист в данной сфере, общался с жуликом онлайн, а Секретная Служба отслеживала их чат в интернет-кафе C&C в Голливуде. В это время в Лос Анджелесе агент пришел в кафе и сел в двух столиках от человека, который заполнял свои фальшивые декларации.

Когда местная полиция и агенты Секретной Службы провели обыск квартиры подозреваемого в Голливуде, они обнаружили, что всё было вычищено: ни компьютеров, ни других улик. Подозреваемый только лишь не перекрасил стены и не почистил ковер. Наниматели Джонсона в Колумбии уже подозревали, что информация об их информаторе стала известна после случившегося на CardersMarket. Теперь у них были все причины полагать, что он предупредил цель о надвигающемся обыске.

Они решили проверить Джонсона на детекторе лжи. Линия на полиграфе оставалась неподвижной, когда Джонсону задали два вопроса: «Выходил ли ты на связь с подозреваемым?» «Выходил ли кто-нибудь другой на связь с подозреваемым?» Джонсон ответил: «Нет». «Нет». Последний вопрос был более развернутым: «Были ли у тебя несанкционированные контакты с кем-либо?» Джонсон снова ответил: «Нет», но его кожа отреагировала резким скачком на диаграмме. Несмотря на запреты агентов, Джонсон продолжал вести беседу с корреспондентом из Нью-Йорк Таймс, он подтвердил, что всерьез собирался заняться написанием книги. Федералы допрашивали его до двух ночи, а затем дали ему на подпись бумагу с соглашением на обыск его квартиры, арендованной агентством.

Обыск квартиры был похож на поиск «пасхальных яиц». Агенты нашли рабочую кредитку в туалете спальни. Записную книжку, спрятанную в туалетном шкафу, в которой хранились номера кредиток, ПИН-коды и данные клиентов. Шестьдесят три кредитные карты были спрятаны в носке, который Джонсон засунул в один из башмаков. Контейнер для завтраков, спрятанный на дне корзины для белья, хранил в свежести две тысячи долларов наличными. И наконец, там же хранились платежные карты Кинко, которыми Джонсон расплачивался за пользование компьютером в местном копировальном магазине.

Он вел тройную жизнь с самого начала вербовки агентством, выставляя себя мошенником в Колумбийском офисе, продолжая вести свою жизнь в оставшееся время. Специальностью Джонсона было то самое мошенничество, что было целью облавы в Лос Анджелесе. Он использовал номера социального страхования из онлайн баз, включая индекс смерти в Калифорнии недавно умерших граждан, затем заполнял налоговые декларации от их имен и получал возвраты средств на созданную заранее карточку, которую он мог обналичить в любом банкомате. На этих махинациях под сорок одним именем он поднял более 130 000 долларов, и всё это под носом Секретной Службы.

Агенты созвонились с поручителем Джонсона и убедили его отозвать залог в 10000 долларов, который освобождал Джонсона из-под стражи. Затем агенты снова поместили Джонсона в окружную тюрьму. Спустя три дня к Джонсону пришел его наниматель с младшим агентом, который не был рад информатору. «Прежде, чем мы начнем, Бретт, я просто хочу сказать, что либо ты говоришь нам все, что ты сделал за прошедшие шесть леть, либо я сделаю все, чтобы отыметь тебя и всю твою семью.» - прорычал агент. «И я говорю не только о текущем положении. Как только ты выйдешь, я буду пресследовать тебя и твою семью до конца твоих дней.»

Джонсон отказался от сотрудничества, таким образом, агентам не оставалось ничего, кроме как начать подготавливать обвинение. Офис прокурора США начал работать над федеральным обвинительным приговором. Однако у мошенника был еще один туз в рукаве. Две недели спустя он сумел восстановить залог, вышел из СИЗО и успешно смылся.

Операция «Рыба-Удильщик» потерпела фиаско. После 1500 часов работы правительство осталось со сбежавшим информатором и десятками тысяч долларов в новой афере. Оставался лишь один лучик надежды: первая партия из двадцати девяти дампов Джонсона, купленная им в мае за шестьсот долларов.

Секретная Служба отследила несколько кредиток в пиццерии Ванкувера, но это был тупик. Однако, корпоративный счет Банка Америки, что использовался при оплате, принадлежал некоему 21-летнему Джону Джианони, проживающему в

Роквилл-центре на Лонг Айленде.

Глава 24. «Обличение»

«Ти, эти девчонки - белый мусор. Лучше не дружи с ними», - сказал Крис, - «Мозги у них другие».

Они сидели в «Наан и Карри», круглосуточном индийско-пакистанском ресторанчике в театральном районе Сан-Франциско. Это произошло спустя три месяца с того момента, когда Ти познакомилась с Крисом и была с ним в одной из его поездок в район Бухты, где он встречал своего таинственного друга-хакера «Сэма», как раз перед рассветом. Они были всего в четырех кварталах от безопасного дома Криса, но Ти до сих пор не была представлена хакеру - ни сейчас, ни до этого. Никто не встречался с Сэмом лично.

Она была очарована тем как все это работало: безналичная природа преступлений и способ, которым Крис организовал свою команду. Он рассказал ей все, когда решил, что она готова, но он никогда не просил ее совершать покупки в магазинах, как остальных. Она была особенной. Он даже не любил болтаться с ней и со своей командой обналичивания одновременно, из опасения, что они как-то могут навредить ей.

Ти также была единственным работником, которому не платят. После того как она отказалась от 40 баксов, оставленных Крисом на ночном столике, он решил, что Ти не возьмет от него никаких денег, несмотря на долгие часы, которые она проводила на Рынке Кардеров и на Русских досках объявлений для преступлений. Крис заботился об аренде дома Ти, покупал ей одежду и оплачивал ее путешествия, но она все же находила такое существование немного странным: жизнь онлайн, путешествия с помощью подтверждений, а не билетов на самолеты. Она стала призраком, ее тело находилось в Оранжевой стране, а разум чаще всего проецировался в Украину и Россию, оказывая поддержку главарям организованной киберпреступности в роли эмиссара Iceman - т.е. мира кардеров Запада.

Она решила, что Iceman был приятно холоден к ней. Он всегда был уважительным и дружелюбным. Когда Крис и его партнер ушли на одно из своих сражений, каждый человек начал скулить и сплетничать Ти о других через ICQ, прямо как дети. С какого-то момента Iceman наговорил ей кучу дерьма и предложил ей уйти в свой собственный бизнес, такой шаг заставил Криса раздражительно попсиховать.

Как-то Крис и Ти болтались в индийской забегаловке; с улицы зашел высокий человек с косичкой и проследовал в глубину зала к кассе, его глаза скользнули по ним всего на мгновение, прежде чем он забрал сумку на вынос и исчез. Крис

улыбнулся: «Это был Сэм.»

Возвращаясь в Оранжевую страну: произведенных фальшивых операций Криса было достаточно, чтобы отправить его детей в частные школы, покрыть апартаменты Ти и в июле начать искать большое и хорошее жилье ему и его семье. Он отправился на поиски дома с Дженноном и в прибрежном городке Капистрано-Бич нашел сдающийся в аренду просторный двухэтажный дом, возвышающийся на утесе над песчаным пляжем в конце тихого дорожного тупика. Там были дружелюбные соседи, висящие над гаражами баскетбольные кольца, и пришвартованная к соседнему причалу лодка. Переезд был назначен на 15 июля.

Дженнон летел обратно на праздники в честь 4 Июля - последний праздник Криса в его старых апартаментах - но вынужден был вернуться назад в дом Ти, пока Крис проводил время с семьей. Это происходило все время; Дженнон должен был лететь в аэропорт Джона Уэйна, рассчитывая потусить в клубах с Крисом, а вместо этого он вынужден был либо скрываться с одной команд, либо побыть нянькой мальчиков Криса у него дома. Ти была довольно терпимой, в отличие от той части дешевых девчонок, обналичивающих карты Криса, но время в квартире Дана Пойнт просто-таки тянулось.

Он позвонил Крису и пожаловался, что ему скучно. «Приходи к дому,» - сказал Крис, они были в бассейне, - «Жена здесь с детьми.»

Дженнон пригласил Ти, которая никогда не видела гостиничного комплекса Криса, расположенного всего в четырех милях от нее. Когда они пришли, Крис, Клара и пара мальчиков плескались в бассейне, наслаждаясь солнышком. Дженнон и Ти сказали привет и расположились на шезлонгах у дома.

Крис остолбенел. «Я смотрю ты привел свою подругу,» - раздраженно сказал он Дженнону.

Клара знала Дженнона, сиделку, но никогда не видела Ти. Она глянула на незнакомку, потом на Дженнона, затем снова на монголку, и тут осознание и гнев перекосили ее лицо.

До Дженнона дошло, что он сделал глупость. Обе женщины выглядели странно похожими. Ти была молодой версией жены Криса, и, судя по первому взгляду, Клара знала, что ее муж спал с этой женщиной.

Крис вытащил себя из бассейна и с нейтральным лицом прогулялся до места где они расположились. Он присел на корточки перед Дженноном, вода с его волос капала на бетон. «Ты что творишь?» - тихим голосом произнес он: «Валите отсюда.»

Они ушли. Впервые, с того момента как она присоединилась к Крису Арагону и его банде, Ти почувствовала себя грязной.

Крис не злился - да он виновен, но он наслаждался как альфа-самец от зрелища Ти и Клары в одном месте. Но все же увлечение Ти становилось проблемой. Он в самом деле по настоящему привязался к ней и ее необычным привычкам, но она становилась нежелательным осложнением.

Он нашел идеальный выход из своего положения. Он просто купил ей билет на самолет в длительный отпуск на ее родину: буквально прогнал свою пламенную любовницу во Внешнюю Монголию.

Пока Крис отвлекался на свою запутанную любовную жизнь, Cardersmarket потреблял все больше времени Макса, он все еще вел свои дела в роли «Digits», бегая. Сейчас он работал в индустрии общественного питания, и это с лихвой окупалось.

Это началось в июне 2006, когда появилась серьезная дыра в безопасности в программном коде RealVNC, «виртуальной сетевой консоли» - программы для удаленного контроля, используемой, чтобы администрировать Windows машины через Интернет.

Ошибка была в короткой процедуре рукопожатия, которая предшествовала каждому установлению новой сессии между VNC клиентом и RealVNC сервером. Критичная часть процедуры рукопожатия наступала, когда сервер и клиент согласовывали тип безопасности применяемый к сессии. Это двухступенчатое рукопожатие. Для начала RealVNC сервер посылал клиенту сокращенный список настроенных для поддержки протоколов безопасности. Список - это просто массив чисел: например, [2, 5] означает, что сервер VNC поддерживает второй тип безопасности, относительно простая парольная схема аутентификации, и тип 5, полностью зашифрованное соединение.

На втором этапе клиент говорил серверу, какой из объявленных протоколов безопасности он хочет использовать, посылая обратно соответствующий номер, как заказ Китайской еды в меню.

Проблема была в том, что RealVNC сервер в первую очередь не сверял ответ от клиента, чтобы узнать был ли он в предоставленном меню. Клиент мог послать обратно любой тип безопасности, даже тот который сервер не объявлял, и сервер безоговорочно принимал его. Даже включая тип 1, который почти никогда не объявлялся, потому что тип 1 означал отсутствие безопасности полностью, это позволяло вам залогиниться в RealVNC без пароля.

Изменить клиент VNC, заставив всегда отсылать тип 1, превращая его в отмычку, было плевым делом. Такой злоумышленник, как Макс мог навести свой взломанный софт на любую коробку с запущенным уязвимым RealVNC и мгновенно насладиться беспрепятственным доступом к машине.

Макс приступил к сканированию на уязвимые инсталляции RealVNC, как только он узнал об этой зияющей дыре. Он ошеломленно наблюдал, как результаты заполняли его экран все ниже и ниже, их были тысячи: компьютеры в домах и в общежитиях колледжей, машины офисов Western Union, банков и вестибюлей гостиниц. Он залогинился наугад в один; и обнаружил себя смотрящим на коридоры через камеры видеонаблюдения, находящиеся в вестибюле замкнутого офисного здания. Другой компьютер был из департамента полиции Среднего Запада, где он мог послушать звонки в 911. Третий перенес его к владельцу дома с системой климат контроля, он поднял температуру на десять градусов и двинулся дальше.

Крошечная часть из всех систем была более интересной и также знакомой благодаря его продолжающемуся вторжению в Pizza Schmizza. Это были ресторанные системы обслуживания. Это были деньги.

В отличие от простых и тупых терминалов, сидящих на прилавках винных магазином и бакалейных лавок, ресторанные системы становились более сложными решениями все-в-одном, которые поддерживали все: начиная с приема заказа и заканчивая рассадкой мест, и все они были под управлением Microsoft Windows. Чтобы поддерживать машины удаленно, поставщики услуг устанавливали их с коммерческими бэкдорами, включая VNC. Со своей отмычкой для VNC Макс мог по желанию открыть многие из них.

Итак, Макс, который однажды сканировал всю военную сеть США, ища уязвимые сервера, теперь целыми днями и ночами фишил своими компьютерами в Интернете, ища и взламывая пиццерии, итальянские рестораны, французские бистро и американские гриль-бары, - он собирал данные с магнитных полос кредиток отовсюду, где их находил.

В соответствии со стандартами безопасности Visa это не должно быть возможным. В 2004 компаниям запретили использовать любые точки продаж, которые сохраняют данные магнитных полос кредиток после завершения транзакций. Чтобы соответствовать стандартам, все основные поставщики сделали патчи, которые позволяют остановить их системы от сохранения данных магнитных полос.

В технике сканирования Макса было несколько взаимодействующих частей. Первая была направлена на поиск установленных VNC, используя быстрый проход «зачистку портов» - стандартный метод разведки, который полагается на открытость

интернета и стандартов.

С самого начала сетевые протоколы интернета были разработаны, чтобы позволить компьютерам совмещать различные типы соединений одновременно - сегодня они могут включать в себя электронную почту, веб-трафик, передачу файлов и сотню других более экзотических сервисов. Чтобы поддерживать все это раздельно, компьютеры устанавливают новые соединения с помощью двух информационных частей: IP адрес машины назначения и виртуальный «порт» на ней же - число от 0 до 65535 - который идентифицирует тип сервиса для требуемого соединения. IP адрес похож на телефонный номер, а порт похож на добавочный номер, который вы вбиваете в коммутатор компании, и потому он может отправить ваш звонок в нужный отдел.

Номера портов стандартизированы и опубликованы онлайн. Софт электронной почты знает, что порт для отправки сообщения 25, веб-браузеры соединяются с 80 портом, чтобы попасть на веб-сайт. Если в соединении на специфичном порту отказано, то это как вызов без ответа, значит сервиса, который вы ищете, нет на этом IP адресе.

Макс интересовался 5900 портом - стандартным портом для VNC сервера. Он настроил свои машины шерстить широкое адресное пространство Интернета, посылая на каждый адрес всего один шестидесяти четырех байтный пакет синхронизации, который проверял, был ли порт 5900 открыт для сервиса.

Адреса, которые отвечали на его фишинг, передавались написанному Максом PERL скрипту, который подключался к каждой машине и пытался залогиниться, используя ошибку в RealVNC. Если эксплоит не срабатывал, скрипт пытался использовать общие пароли: 1234, vnc или пустую строку.

Если он попадал внутрь, программа вытаскивала некую предварительную информацию о компьютере: название машины, а также разрешение и глубину цветов монитора. Макс пренебрегал компьютерами с низким качеством дисплеев, предполагая, что они были домашними компьютерами, а не для бизнеса. Эта операция была очень быстрой: Макс запустил ее на пяти или шести серверах сразу, каждый из которых просматривал сеть класса В, около шестидесяти пяти тысяч адресов, за пару секунд. Таким образом его список установленных уязвимых VNC рос примерно на десять тысяч записей каждый день.

Системы точек продаж были иголками в огромном стоге сена. Он мог определить несколько просто из названия: «Aloha» означает скорее всего терминал Aloha POS, произведенный в Атланте на базе системы от Radiant Systems, его излюбленной цели; «Maitre‘D» был конкурирующим продуктом от Posera Software из Сиэтла. Для

остальных же требовалось догадываться. Любая машина с названием «Server», «Admin» или «Manager» требовала повторного взгляда.

Проскальзывая через свой VNC клиент, Макс мог видеть экран компьютера, как если бы он сидел перед ним. Т.к. он работал ночью, дисплей бездействующего PC был обычно темным, потому он не навязчиво толкал мышь, останавливая тем самым заставку. Если же кто-то был в комнате рядом, это могло выглядеть немного жутковато: помните то время, когда монитор вашего компьютера загорался без причины, а курсор дергался? Это мог быть Макс Вижн, быстро кидающий взгляд на ваш экран.

Эта часть проверки была медленной. Макс нанял Ти помогать - он дал ей VNC клиент и начал скармливать ей списки уязвимых машин, заодно скинув инструкции по тому, что надо искать. Вскоре Макс был подключен к закусочным по всей Америке. Бургер Кинг в Техасе. Спорт-бар в Монтане. Модный ночной клуб во Флориде. Калифорнийский гриль-бар. Он двинулся в Канаду и нашел еще больше.

Макс начинал свои продажи краденных дампов с одного единственного ресторана. Теперь же у него было целых сто, подающих ему данные кредитных карт почти в реальном времени. У Digits будет намного больше работы.

С таким большим объемом работы Дэйв «Эль Мариачи» Томас выбрал плохое время, чтобы стать настоящей болью в заднице Iceman‘а. В июне Томас сделал что-то почти неслыханное в узком кругу компьютерного подполья: он вынес беседы с форумов на публику, в обычное киберпространство, атакуя таким образом Cardersmarket в комментариях широко читаемого блога по компьютерной безопасности, где он обвинял Iceman‘а в связи с «ОП» (органами правопорядка).

«Вот сайт, размещенный в Форт-Лодердейле, штат Флорида,» - писал Томас, - «Фактически он расположен в чьем-то доме. Тем не менее ОП отказывается закрыть их. Несмотря на то, что этот сайт продает PIN коды и номера PayPal, eBay и так далее, ОП все это время смотрит на других игроков.»

«ОП утверждают, что они ничего не могут сделать с сайтом размещенным на территории США. Но, по правде говоря, ОП сами запустили этот сайт точно также, как они это сделали с Shadowcrew.»

Подчеркивая договоренности размещения Рынка Кардеров, Томас целился в Ахиллесову пяту Iceman‘а. Сайт до сих пор продолжал мирно мурлыкать потому, что в компании Affinity до сих пор не замечали незаконный сервер среди десяти тысяч своих законных сайтов. Эль работал над тем, чтобы изменить такой расклад, снова и снова подавая жалобы в компанию. Такой тактике не доставало логики: если Cardersmarket действительно был под контролем правительства, то жалобы летели в

глухие уши; только если бы это был по-настоящему преступный сайт, Affinity бы его удалила. Если бы Iceman утонул, это бы значило что он не ведьма.

Неделю спустя после поста Томаса, Affinity резко обрубила Cardersmarket. Закрытие рассердило Макса, у него бы была хорошая штука в ValueWeb. Ну что ж, ему пришлось искать новый зарубежный легитимный хостинг, который мог быть противопоставлен Эль Мариачи, в компаниях, находящихся в Китае, России, Индии и Сингапуре. Это всегда выходило одинаково - они б запросили немного денег авансом как стоимость входа, а потом бы раскатали красную ленточку перед парадной дверью, при этом спросив паспорт и лицензию на предпринимательскую деятельность или корпоративные документы.

«Это не прокатит потому, что у тебя немного ИДИОТСКИ ТУПОЕ НАЗВАНИЕ, говорящее «здесь КАРДЕРЫ» или «это РЫНОК КАРДЕРОВ». Ну так что, возможно?» - писал Томас, дразня Iceman‘а, - «Может если б ты не кричал «ЗДЕСЬ РАБОТАЮТ КАРДЕРЫ», то ты мог бы иметь маленький работающий сайт с возможностью его дальнейшего роста до того монстра, в котором ты отчаянно нуждаешься.»

Сейчас это было личным: Томас ненавидел Iceman‘а, независимо был ли он федералом или нет, и это чувство становилось взаимным.

Наконец, Макс забрался в Staminus, Калифорнийскую фирму, специализирующуюся на хостинге с высокой пропускной способностью для защиты от DDoS атак. К тому времени Томас рвал и метал в него в комментариях одного случайного блога под названием «Жизнь на Дороге.» Блогер процитировал комментарии Томаса о Рынке Кардеров в краткой заметке о форумах, невольно превращая свой блог в новое поле боя в войне Эль Мариачи против Iceman.

Iceman подобрал перчатку и разместил длинное публичное опровержение против осуждений Томаса, обвиняя своего врага в «лицемерии и клевете».

> СМ - не «доска объявлений для преступности» или «империя», или любая другая подобная этой обвиняемая всеми ерунда. Мы просто форум, который выбрал возможность позволить обсуждать финансовые преступления. Мы также предоставляем право в суждении, кто из участников настоящий, а кто подделка, но все это только наши мнения, мы не делаем на этом денег. Мы только НОСИТЕЛЬ информации, мы ФОРУМ, через который эта связь может проходить без притеснений. СМ вообще не вовлечен ни в какие преступления. Управлять форумом и позволять обсуждать не является незаконным.

> На craigslist.com есть личности, дающие объявления о проституции, наркотических соединениях и других очевидных преступлениях, но люди пока не зовут craigslist «универсальным магазином шлюх и драгдилеров» или преступной империей. Он расценивается как НОСИТЕЛЬ, который не отвечает за содержание постов на нем. Такова позиция Рынка Кардеров.

Смелая оборона полностью игнорировала факт наличия на Рынке Кардеров детальных руководств к преступлениям и обзоров систем, не говоря уже о скрытой составляющей сайта: дающей Максу площадку для продаж украденных данных.

Зная что его Калифорнийский хостинг не удовлетворит подполье, Макс продолжил свои поиски за рубежом. Уже в следующем месяце он взломал для себя новый сервер, на этот раз в стране, которая была настолько далеко от США, как никто другой в Сети; в стране, которая вряд ли ответит на жалобы Дэйва Томаса или даже Американского правительства.

«Cardersmarket теперь находится в ИРАНЕ,» - 11 августа объявил он, - «Регистрация возобновлена.»

Глава 25. «Захват территории»

> В войне самое главное — быстрота: надо овладевать тем, до чего он успел дойти; идти по тому пути, о котором он и не помышляет; нападать там, где он не остерегается.

«Искусство войны» Сунь Цзы было настольной книгой Макса. Сидя в своём тайном убежище, он набросал план наступления. Было пять англоязычных подпольных кардинговых сайтов, и четыре из них были лишними. Недели ушли на изучение противника: ScandinavianCarding, Vouched, TalkCash и, его главный враг, — DarkMarket. Этот английский сайт появился на месяц раньше CardersMarket и прилагал большие усилия, добиваясь репутации зоны, защищенной от взлома.

В известном смысле, планы Макса проникнуть на другие площадки, строились на его положительных качествах. На руку ему играло, что он не был жадным, и что он делал бизнес на CardersMarket. Теневая кардинговая сцена была разрушена, а когда Макс сталкивался с чем-то разбитым, он не мог отказаться восстановить это, совсем как делал это несколько лет назад для Пентагона.

Играло свою роль и самолюбие. Казалось, весь кардинговый мир думал, что Iceman всего лишь администратор, способный только устанавливать ПО. Макс видел прекрасную возможность показать кардерам, как они ошибались.

На DarkMarket нашлось слабое место. Британский кардер JiLsi пользовался этим сайтом. Он использовал один и тот же пароль: “MSR206” везде, включая и CardersMarket, где Макс имел доступ ко всем паролям. Теперь Макс мог проникнуть и хозяйничать на DarkMarket.

А вот Vouched был крепостью, вы даже не могли зайти на сайт без доверенного цифрового сертификата, установленного на вашем браузере. К счастью JiLsi был зарегистрирован и здесь, и даже имел модераторские права. Макс нашел копию доверенного сертификата на одном из почтовых аккаунтов JiLsi, который был защищен обычным паролем “MSR206”. Теперь оставалось лишь зайти на Vouched как JiLsi, и вся база данных была доступна.

Макс установил, что поиск по сайту на TalkCash и ScandinavianCarding был уязвим для атаки SQL injection. Макс не был в этом деле первооткрывателем. Уязвимость к такой атаке — обычное дело для сайтов.

SQL injection использует архитектуру сложных по своей структуре сайтов. Когда вы заходите на веб-сайт с динамическим содержимым: новостными заметками, записями в блог, биржевыми котировками, на сайты интернет-магазинов программное обеспечение (ПО) сайта предоставляет информацию, извлекаемую из базы данных. Эта база данных обычно находится на другом компьютере, а не на хосте, к которому подсоединен ваш компьютер. Веб-сайт — это фасад, а сервер с данными — заблокирован. В идеале, он вообще не доступен из интернета.

Программное обеспечение сайта общается с сервером, хранящим данные, на языке SQL (Structured Query Language язык структурированных запросов). К примеру, команда SELECT запрашивает у сервера всю информацию, которая подходит под определенные критерии. INSERT добавляет информацию в базу данных. Редко используемая инструкция DROP удаляет большие объёмы данных.

Это опасный инструмент, потому что зачастую ПО должно отправить запрос посетителя сайта, как часть SQL- команды серверу. Если посетитель сайта напишет в строку поиска: Sinatra, ПО сайта запросит у сервера информацию следующим образом:

```
SELECT titles FROM music_catalog
WHERE artist = ‘Sinatra’;
```

SQL injection случается, когда ПО неправильно обрабатывает запрос пользователя перед передачей его в виде команды серверу. Пунктуация может сбить ПО с толку. Если в выше приведённом примере написать в строку поиска сайта: `Sinatra’; DROP music_catalog;` обратите внимание на апостроф и на точки с запятыми, из-за них сервер получит команду в виде:

```
SELECT * FROM music_catalog
WHERE artist = ‘Sinatra’; DROP music_catalog;’;
```

Для базы данных это две последовательные команды, разделенные точкой с запятой. Первая найдет альбомы Синатры, вторая — удалит музыкальный каталог.

SQL injection обычное оружие в арсенале хакера. Даже сегодня таким образом проникают на сайты всех уровней, в том числе сайты электронной коммерции и сайты банков. Итак, в 2005 ПО TalkCash и ScandinavianCarding оказались под прицелом.

Чтобы воспользоваться уязвимостью TalkCash, Макс зарегистрировался, и послал

невинное на вид сообщение. В теле сообщения скрывалась SQL команда, написанная шрифтом, цвет которого совпадал с цветом фона, а потому невидимая глазу. Он ввел поисковый запрос, а ПО сайта передало скрытую команду в базу данных, где она была выполнена. Эта команда была INSERT, и она добавила на сайт еще одного администратора — Макса. То же самое он проделал и на ScandinavianCarding.

К 14 августа Макс был готов показать миру кардинга, на что он способен. Он проник на сайты через тайно проделанные дыры, и, используя свою поддельную учетную запись администратора, скопировал базы данных. Такой план был достоин Сунь Цзы: никто из конкурирующих площадок не ожидал атаки и захвата. Большинство кардеров избегало публичности, не выставляло себя на показ. Враждебный захват был беспрецедентен.

Покончив с англоязычными сайтами, Макс переключился на Восточную Европу. Было стремление объединить Восточноевропейских кардеров с западными, но усилия Ти были бесплодны. Русским нравился американская Ти, но они ей не доверяли. Дипломатия провалилась, настало время действовать. Он обнаружил, что такие площадки, как Cardingworld.cc и Mazafaka.cc защищены не лучше, чем западные, и вскоре уже скачивал оттуда приватную переписку и статьи с форумов. Мегабайты кириллицы уплыли на его компьютер. Тайны жульнических операций, рассказы о хакерских атаках, которые велись против Запада и продолжались месяцами, теперь получили постоянную прописку на жёстком диске Макса в районе Тенделойн, Сан-Франциско.

Завершив скачивание базы данных, на каждом сайте он запускал команду DROP, стирая оригинал. ScandinavianCarding, TalkCash, Vouched, DarkMarket, Cardingworld — все эти хлопотливые, круглосуточные торговые площадки, которыми пользовались около 10 тысяч человек, обслуживавшие теневую экономику и ворочавшие миллиардами долларов, прекратили своё существование. Шестизначные суммы криминальных структур; деньги на расходы, выданные детям, женам или любовницам; взятки полицейским; ипотечные суммы, дебетовые счета, платежи — всё это в мгновение ока исчезло. Неотвратимо. Деньги утеряны. Всем им предстояло узнать имя Iceman.

Макс продолжил работу с украденной информацией, игнорируя Восточноевропейские данные. После удаления дублирующихся и нежелательных записей с четырех англоязычных площадок, осталось 4500 новых членов для CardersMarket. Всех их он добавил в базу данных своего сайта, так что теперь они могли войти на него, используя свои старые логины и пароли. На CardersMarket теперь было шесть тысяч пользователей. Больше, чем на Shadowcrew когда-либо.

Он объявил о силовом слиянии в массовой рассылке своим новым членам. Когда в Сан-Франциско наступило утро, он увидел их всех вместе, смущенных и яростных, на своём объединённом форуме. Matrix001, немецкий администратор DarkMarket требовал объяснений у Iceman‘а.

Обычно молчаливый король спама Master Splyntr принялся критиковать организацию материалов, похищенных Iceman‘ом. Все содержимое сайтов-конкурентов теперь размещалось в новом разделе CardersMarket, который назывался «История записей с поглощённых форумов.» Эти записи были не отсортирован и было трудно что-либо найти; Макс считал, что эта информация заслуживает сохранения, но не сортировки. Поначалу Макс наблюдал со стороны, затем вступил в беседу и дал понять, кто за всем этим стоит.

> @Master Splyntr: «Если у вас нет ничего конструктивного или нового, ваш комментарий нежелателен. Если вам не нравится организация выкладки, проваливайте и возвращайтесь позже, потому что она еще не отсортирована.»
>
> @matrix001: «Старые форумы были небрежны в вопросах безопасности, используя общие хостинги, отказываясь от шифрования данных, входя в систему по IP адресам, используя 1234 как административный пароль (да, действительно, это так!) и вседозволенность администраторов. Некоторые, такие как Vouched, давали ложное чувство безопасности, что, как вам известно, ещё хуже.
>
> Вы спросите, что всё это значит? Если вы имеете в виду слияние пяти кардинговых форумов вместе, то короткий ответ таков: потому, что у меня нет ни времени, ни желания присоединить ещё четыре оставшихся из девяти. По существу этот шаг назрел. Зачем иметь пять форумов с одинаковым содержанием, разделением продавцов и покупателей, со слабой безопасностью, слабым администрированием, слабой модерацией. Это не просто так, это для всех благо. С правильной модерацией мы вернёмся к изначальному „жёсткому“ руководству с нетерпимостью к риппингу и анархии в обсуждении тем и промо-акций. Сейчас много мусора со старых форумов, но мы его вычистим.
>
> Ради чего? Безопасность. Удобство. Повысить качество и уменьшить помехи. Привнести порядок в бардак…»

Канадский хакер Silo заявил, что Iceman разрушил социальные связи, что держали

сообщество кардеров вместе. Он погубил доверие.

> Silo: «Ты угробил безопасность нашего сообщества. Украл данные с других форумов. Могло бы твоё слияние случиться при согласии администраторов всех форумов? В чём разница, если я взломаю твою почту и прочитаю её или опубликую на форуме? С какой стороны ни посмотри, ты показал как мало следует доверять в нашем сообществе. Моё предложение следующее: ты должен удалить данные, которые украл. Правильно будет СПРОСИТЬ администраторов площадок; правда ли, что единая площадка отвечает интересам нашего сообщества; и подождать, что они ответят. Вот моё мнение.»
>
> Людей с навыками Iceman‘а много. От общества зависит, как они используют их.

Vouched вернулся онлайн, но ненадолго. Предполагалось, что это приватный, безопасный форум, открытый только для избранных. После проделки Макса доверие к нему пошатнулось, и никто не захотел возвращаться. ScandinavianCarding и TalkCash были обречены, у них не было резервных копий баз данных. В основном их клиенты остались на CardersMarket.

Кроме русских форумов, которые Макс не мог использовать из-за незнания языка, триумф Макса омрачало только одно: DarkMarket. Его главный соперник имел резервные копии и занялся восстановлением, обещая вернуться к работе через несколько дней. Это был вызов всему, что Макс пытался достигнуть для себя и для сообщества. Война началась.

Тем временем, в графстве Оранж, Крис тоже укрупнял свой бизнес. Он решил, что было бы удобно, чтобы все сотрудники, занятые полный рабочий день, жили в одном месте. Комплекс квартир Архстоун, сдававшийся в аренду через интернет, прекрасно вписывался в его планы. Желающие могли заполнить заявку на сайте компании, внести задаток $99 и плату за первый месяц картой. Крис всё мог сделать через интернет, и его сотрудники могли не показываться до дня въезда, когда им следовало появиться в офисе арендодателя, предъявить свой ID и получить ключи от квартир. Он отправил двух своих сотрудников и Маркоса, своего связного в Архстоун Мишн Вьехо — меблированные комнаты в виде особняков, раскрашенные в цвета заката и прилегающие к холму, усеянному пальмами и высоковольтными линиями, в пяти минутах ходьбы от его дома. Также он хотел увеличить свою команду. Одна сотрудница уехала в Толедо после вторичного банкротства её магазина, а две другие с омерзением отказались работать, когда подруга-тинэйджер Криса забеременела от него. Сейчас он платил за квартиру

молодой мамаши и их сына, чьё существование скрывал даже от своей матери.

В офисе НСФТА (NCFTA) в Питтсбурге Кейт Муларски, писавший под именем Мастера Сплинтера, получил тайное сообщение от Iceman‘а два дня спустя после захвата. Хакер извинялся за некоторые необдуманные слова на форуме. Ожидая следующий этап противостояния DarkMarket и CardersMarket, Iceman похвастал, что легко отразит любую DDoS атаку на свой сайт. Позднее, поискав в интернете информацию о Мастере Сплинтере, он узнал, что это спамер с мировым именем и армией ботов. Кажется Iceman невольно сделал из простого критика непримиримого врага.

> Не обижайся на мои комментарии. Это правда, что если кто-либо попытается напасть на мой сайт, я отслежу его и поддену или завалю. Но я не хотел бросить вызов. Никому не хочется терять время на такие дела, по настоящему DDoS не приносит радости и поэтому, пожалуйста, не принимай неверных решений :-)

Муларски начал понимать, что перед ним открываются новые возможности. Никто никому больше не доверял. Все обозлились на всех. Если он сыграет за обе стороны, то сможет устраивать набеги на территорию обоих администраторов, пока они сцепятся в битве за пользователей. У него было три независимых аккаунта. Он воспользовался одним, чтобы ответить.

> «Никаких проблем, бро, мы — команда. Я сам могу чего ляпнуть сгоряча. Зачем мне атаковать. Черт, мои боты даже еще не настроены для атаки. Рассылки приносят мне гораздо больше. Я не делаю ничего, что не приносит доход. Только если мне не объявят вендетту, которой пока нет. И если тебя атакуют, я также хорош в отслеживании и нападении, постучись ко мне в ICQ 340572667, если будет нужна помощь :-) MS»

Муларски сидел перед монитором, ожидая ответа. Через несколько минут на экране появилась надпись:

> «Огромное спасибо :-), кстати, есть у тебя соображения по ведению дел, помимо банальных советов по организационным моментам? Я собираюсь внести изменения и ты теперь можешь предлагать услуги и можешь выбрать себе любой ник. Не знаю предоставляешь ли ты услуги электронной почты, но думаю, что иметь свою сеть круто.

> Уверен, что нам лучше иметь возможность нанять тебя. Также, если ты понёс убытки в бизнесе, приношу свои извинения. Я сохранил некоторых вендоров, но часть была утеряна. Просто довожу до твоего сведения. Спасибо, бро :-) Также добавил тебя в группу VIP.»

Это был многообещающий ответ. Муларски обсудил все со своим инспектором. Затем обратился в штаб-квартиру к руководству Группы II. На две ступени ниже «участия под прикрытием» от ФБР, но на ступеньку выше его роли «пассивного наблюдателя». Его положение не позволило бы ему участвовать в каких-либо незаконных делах, но он мог бы наконец активно бороться с подпольем. Он назвал CardersMarket, и все связанное с работой площадки, стало предметом расследования.

Разрешение пришло быстро. Но, несмотря на обнадёживающие слова, Iceman проверял сомнительного партнёра; он держал Муларски на расстоянии, не делился секретами и только переписывался в чате через сайт. Агенту ФБР больше повезло на другой стороне. Он был одним из первых членов DarkMarket и после непродолжительных переговоров JiLsi, основатель сайта, быстро принял Мастера Сплинтра на должность руководителя. В начале сентября Сплинтр стал модератором сайта.

Война разгоралась. Несмотря на уроки августовского вторжения, JiLsi не мог добиться полной защиты DarkMarket. Iceman стал регулярно проникать в базу данных и удалять случайные аккаунты, просто, чтобы досадить JiLsi. Когда DarkMarket в ответ начал яростную DDoS атаку против Иранского хоста CardersMarket, Iceman ответил тем же. Оба сайта затрещали под напором ненужных пакетов. Iceman втайне арендовал место у американской хостинговой компании с широким каналом, пропустив трафик через них, очистив, он пересылал его дальше, на свой настоящий сервер по зашифрованному каналу. JiLsi рвал волосы, делился своими бедами с Мастером Сплинтером. Муларски переместил своё внимание с Iceman‘а на босса Британских кибер-преступников, который начал обращаться с ним как с другом. Он догадался, что JiLsi задумался кому бы доверить на время DarkMarket, чтобы сделать неуязвимый хостинг. Кому-то, кто привык поддерживать работу сайта, который ненавидят все. Спамеру.

«Ну, ты знаешь, на что я способен,» — написал он в чат, — «Я хорош в создании серверов, я охраняю их круглосуточно. Я могу сделать это для тебя.»

Муларски задумал оригинальный план. В прошлом и у «Секретной службы», и у ФБР были администраторы информаторы: Альберт Гонсалес на ShadowCrew и Дейв Томас на Grifters. Но реально работать на площадке, дало бы доступ ко всему от IP

адресов кардеров, до любой секретной информации. Если бы Мастер Сплинтр занялся сайтом, он получил бы такое доверие, о котором ни один агент не мог и мечтать. JiLsi заинтересовался предложением Мастера Сплинтра, и Муларски приготовился к следующей поездке в Вашингтон, Округ Колумбия.

Глава 26. «Что в Вашем бумажнике?»

Продажа 100% проверенных свежих дампов (США), скидки:
$11 MasterCard
$8 Visa Classic
$13 Visa Gold/Premium
$19 Visa Platinum
$24 Visa Signature
$24 Visa Business
$19 Visa Corporate
$24 Visa Purchasing
$19 American Express = снижение цены (было 24)
$24 Discover = снижение цены (было 29)
Минимальный заказ - 10 штук.
Продажа по типам карт. Не по BIN'ам.

Агрессивный захват, провернутый Максом был совершен с целью объединить силы коммьюнити, а не с целью персонального обогащения. Тем не менее, его бизнес по продаже краденных данных с магнитных полос пластиковых карт после объединения форумов процветал как никогда - он получал порядка тысячи долларов в день, продавая дампы кардерам по всему миру, в дополнении к пяти - десяти тысячам, что он получал от партнерства с Крисом.

На публике, во время встреч ФТК (Федеральная Торговая Комиссия) или где бы то ни было, индустрия кредитных карт изо всех сил старалась скрыть последствия учащающихся фактов кражи данных с магнитных полос по всему миру. Visa, лидер в сфере кредиток, поддержал финансируемый промышленностью отчет компании Javelin Strategy and Research, которое обвиняло в сложившейся ситуации клиентов, а не компании - источники слива данных кредиток и краж персональных данных: 63% произошедших случаев обусловлены потерей или кражей кошелька с последующей кражей данных доверенными партнерами, кражей электронной почты и исследованием содержимых мусорных контейнеров.

Доклад был весьма обманчив - велся только подсчет случаев, в которых жертва была в курсе каким способом была украдена информация. Частные данные компании Visa говорили о реальном состоянии дел. Украденные кошельки не были

основным источником мошенничества с середины 2001 г. - кража данных карты с сайтов электронной коммерции била все рекорды роста среди других типов мошенничества с картами, выдавая при проведении транзакции по телефону или в интернет в качестве результата фальсификацию - «не предоставлена информация по карте».

В 2004 г., когда украденная с магнитных дорожек информация стала массовым товаром в андерграунд коммьюнити убытки по поддельным картам выросли с такой же стремительностью. В первом квартале 2006 подделка карт в стиле Криса Арагона выбила с первого места вид мошенничества card-not-present, превысив $125 млн ежеквартальных потерь банков-партнеров Visa.

Почти все эти потери были связаны с появлением прейскурантов как у Макса. На форуме Carders Market росло количество страниц с положительными отзывами о продавце Digits и, конечно, росла его репутация как честного торговца. Это было предметом гордости Макса и знаком отличных от большинства нравственных ценностей, что было присуще ему с детства. Макс мог с огромным удовольствием взломать кардера и скопировать всю хранившуюся на его жестком диске информацию, но если клиент заплатил ему за информацию, то он даже не рассматривал вариант какого либо вмешательства.

Щедрость Макса тоже была в почете. Если у Макса были дампы с близящимся к завершению сроком годности, то он предпочитал отдавать их бесплатно, а не оставлять лежать без дела. Примерное ведение бизнеса и качество продаваемого продукта вывели Макса в пятерку лучших дамперов в мире, хотя обычно на рынке доминировали продавцы из Восточной Европы.

Макс был осторожен с процедурами автоматической продажи. Отказываясь продавать дампы по BIN'ам (bank identification number, идентификатор банка-эмитента) он утяжелял работу федералам: правительство не могло просто купить двадцать дампов, относящихся к одному и тому же финансовому институту и попросить банк проверить общую точку покупки по транзакциям. Вместо этого все заинтересованные лица должны были тесно сотрудничать друг с другом для того чтобы выявить источник.

Помимо этого, только несколько наиболее доверенных соратников знали, что Digits и Iceman это одно и то же лицо - в большинстве это были админы, например, как Крис, канадский кардер под псевдониму NightFox и новый член команды под ником Th3C0rrupted0ne.

Со всеми людьми со сцены, что встречался Макс только Th3C0rrupted0ne имел примерно схожее прошлое хакинга. Будучи еще подростком C0rrupted обнаружил сцену с варез контентом в системах электронных досок объявлений,

коммутируемую dial-up модемом, а затем занялся хакингом для развлечения, встав под начала Acid Angel, -null- и прочих хакеров. Он дефейсил сайты для развлечения и присоединился позже к группе хакеров Ethical Hackers Against Pedophiles - vigilante gray hats (Этичные хакеры против педофилов - добровольцы в серых шляпах), которые боролись с детской порнографией в интернете.

Так же, как и Макс ранее он считал себя хорошим парнем, пока не стал Th3C0rrupted0ne.

Если говорить про другие черты - у них не было ничего общего. Продукт трудного детства в большом городе спальной застройки C0rrupted стал наркоторговцев в раннем возрасте и получил первый срок, за ношение оружия, еще в 1996 г., когда ему было 19 лет. В колледже от начал делать поддельные удостоверения личности для друзей и как-то раз его интернет исследование вывело его на Fakeid.net - электронная доска объявлений, где такие эксперты как ncXVI начинали свою деятельность. Он закончил университет, получив возможность устроиться на низкооплачиваемую работу и заниматься мошенничеством с кредитными картами, как раз в то время, когда Shadowcrew прекратила своё существование, а затем поиски привели его к наследникам прекратившей существования доски.

Дипломатичность и спокойствие C0rrupted повсеместно нравились участникам сцены и он наслаждался модерскими или админскими привилегиями, что ему давали на большинстве форумов. Макс поручил ему позицию администратора на Carders Market летом 2005 г. и сделал его неофициальным представителем после враждебного поглощения. Примерно спустя неделю после того, как C0rrupted занялся полномочия админа Макс посвятил его в свой секрет о том, что и Iceman, и Digits, оба этих псевдонима, принадлежат Максу.

> Очевидно же, что Digits - это тоже я. Мог бы сказать это прямо после того, как я спалился в ICQ (говоря о нашем «форуме» и прочих вещах).
>
> Вообще это довольно большая заноза в заднице - держать это в тайне от людей, которых я знаю и которым я доверяю, например, от таких, как ты. Вот как-то так …
>
> В любом случае, разница такова, что Iceman полностью в рамках закона. Digits - наоборот, нарушает его. Я считал, что если я смогу разделить две деятельности таким образом, то не будет никакой легальной опоры на которую можно будет опереться, заняв позицию администратора после «меня».

Крис оставался наибольшей угрозой для безопасности Макса. Каждый раз, когда они сталкивались лбами Макс помнил о том, что он уязвим и он имеет дело с единственным кардером, который знает его в лицо и причастен к его реальной личной жизни. «Я не могу поверить, как много ты знаешь обо мне» - выдавил он, со злобой на самого себя.

Тем временем Крис пытался приобщить Макса к идее о том, что им нужно заняться чем-то серьезным, сорвать куш, что заставит их выйти из криминального бизнеса и заняться чем-то легальным, как вариант, основать новый легальный стартап для Криса в округе Ориндж. Он сделал диаграмму и пошаговый план для обоих и назвал его «Список виртуозов».

Предполагалось, что Макс проникнет в банковскую сеть и получит возможность перевести миллионы долларов на счета, которые даст Крис. Он должен довести до конца то, чем он занимался с самого начала их партнерства, с того самого времени, когда он работал из гаража Криса, когда он взламывал маленькие банки, счета и займы. Он обладал доступам к сотням таких счетов и займов и мог перевести деньги со счетов клиентов - нужно было лишь только желание. Но финал схемы завис в разработке по вине Криса. Он должен был найти безопасное пристанище для денег, что украдет Макс - какое-нибудь оффшор-хранилище, куда они могли бы перевести деньги без риска, что пострадавший банк отзовет перевод. Пока ему это не удавалось.

Таким образом, в сентябре, когда Макс обнаружил критическую уязвимость нулевого дня в новом Internet Explorer он поделился этой новостью не с Крисом, а с другим партнером, который обладал большими познаниями в международных финансах - администратором Carders Market под ником NightFox.

Брешь в безопасности была катастрофическая - еще одно переполнение буфера, на этот раз задуманное для отрисовки векторной графики на стороне клиента. К сожалению для Макса, хакеры из Восточной Европы нашли уязвимость раньше него и уже во всю пользовались ей. Компания компьютерной безопасности уже обнаружили эксплойт от русских хакеров, который заражал компьютеры при посещении порно сайтов и отправили его в Microsoft. Департамент внутренней безопасности издал довольно тупое предписание для пользователей IE - «Не открывайте нежелательные ссылки».

Уязвимость была известна, но патча еще не было. Все пользователи IE были уязвимы. Макс получил эксплойт русских хакеров ранним утром 26 сентября и с нескрываемым энтузиазмом поспешил поделиться им с NightFox.

«Предположим, что мы получим бесплатный билет на аттракцион - поимей любую компанию сегодня», Макс написал в системе обмена сообщениями Carders Market.

«Ок, пожалуйста. Никаких ограничений. visa.com. mastercard.com. egold.com. Любой электронный ящик сотрудников для любых целей. Google. Microsoft. Не важно. Всех можно поиметь хоть прямо сейчас.»

Microsoft выпустил патч позднее в тот же день, но Макс знал, что даже компаниям, относящимся к безопасности со всей серьезностью понадобятся дни или недели на установку обновления на все компьютеры сотрудников. Русский эксплойт уже был обнаружен антивирусными программами, поэтому он внес в него изменения, чтобы их сигнатуры отличались и прогнал через свою антивирусную лабораторию чтобы убедиться в отсутствии возможности обнаружения.

Единственное что оставалось - социальная инженерия - Максу нужно было обмануть свои цели чтобы они посетили веб-сайт с эксплойтом. Макс остановился на выборе доменного имени financialedgenews.com и разместил его у хостинг провайдера ValueWeb.

NightFox вернулся со списком целей - CitiMortage, GMAC, Experian's Lowermybills.com, Bank of America, Western Union MoneyGram, Lending Tree и Capital One Financial - один из самых крупнейших эмитентов кредитных карт в стране. У NightFox были обширные базы с внутренними адресами сотрудников компаний, которые он получил от компании «конкурентная разведка» и он отправил Максу тысячи адресов каждой компании, на которую они нацелились.

29 сентября Макс зарядил в свой спам софт адреса и начал выстреливать персонализированным письмом в своих жертв. Отправителем письма числился «Gordon Reily», с обратным адресом g.reily@lendingnewsgroup.com.

> Я репортер Lending News и я расследую недавнюю историю о утечке данных клиентов Capital One. Я заметил упоминание имени Mary Rheingold в статье в Financial Edge и хотел бы договориться о интервью для освещения больших подробностей в новой статье.
>
> http://financialedgenews.com/news/09/29/Disclosure_Capital0ne
>
> Я буду очень признателен если Вы найдете время для дальнейшего обсуждения деталей вышеупомянутой статьи.

Каждая копия письма была персонализирована, поэтому каждый сотрудник будет думать, что именно его или её имя упомянуто в статье Financial Edge. В Capital One, 500 сотрудников, начиная от руководителей и заканчивая PR представителями и ИТ специалистами получили сообщение. Примерно 125 из них перешли по ссылке и

были переправлены на станицу с обычной сводкой финансовой индустрии. В то время как они ломали голову над страницей, скрытый эксплойт просочился через корпоративный брандмауэр на их машины.

Эксплойт открыл бекдор, позволяющий Максу на досуге проскользнуть на жесткие диски жертв и порыться в поисках конкурентной информации, проанализировать внутренний банковский трафик и украсть пароли. Это не сильно отличалось от того, что он делал с тысячами компьютеров Министерства обороны много лет назад. Тогда, когда это было простое озорство из-за любопытства.

Глава 27. «Первая сетевая война»

Кейт Муларски стоял у подиума, презентация заполняла собой весь ЖК экран позади. Перед ним сидели, собравшись вокруг стола в конференц-зале, пятнадцать высокопоставленных представителей ФБР и специалистов министерства юстиции. Все они были сосредоточены. Муларски предлагал им нечто новое, и такого им раньше никогда не доводилось делать.

Авторизация первого уровня была для бюро редким делом. В первую очередь Муларски написал двадцатистраничный документ, раскрывая все аспекты плана и собирая юридические оценки от сотрудников ФБР по каждому из них. Генеральный совет агентства был воодушевлен открывавшимися перспективами: одобрение плана создавало прецедент, приемлемый и для будущих операций под прикрытием в сети.

Главным препятствием для комитета по оценке подобной деятельности в минюсте был вопрос ответственности за то, что на сайтах под управлением правительства США позволялось совершаться преступлению. Вопрос стоял следующий: как же Муларски смягчит этот вред как сделать так, чтобы невинные люди и организации не пострадали. Ответ был готов: преступная деятельность на DarkMarket будет продолжаться, с участием ФБР или без. Однако, если Бюро будет контролировать сервер, а Мастер Сплинтер управлять сайтом, ФБР сможет пресечь распространение значительной части украденных данных, которые бы иначе свободно проходили через черный рынок. Документ предполагал, что любые финансовые данные будут сразу направлены в пострадавшие банки, и в результате украденные кредитные карты смогут быть заблокированы раньше, чем их используют.

Встреча продлилась 20 минут. Вернувшись в Питтсбург седьмого октября, Муларски дал добро на овладение DarkMarket. Айсмен все еще числился мишенью для операции, но главными целями стали JiLsi и другие лидеры сайта.

Когда его жена ушла спать, Муларски устроился перед диваном, включил телевизор и написал JiLsi в ICQ. После обмена безобидными шутками они перешли, наконец, к делу. DarkMarket снова находился под DDoS-атакой, а Муларски, под псевдонимом Мастер Сплинтер, был готов перенести сайт на защищенный сервер. JiLSi должен был лишь сказать одно слово, и проблемы с Айсменом бы ушли в прошлое.

У JiLsi обнаружились некоторые опасения, ведь DarkMarket был его детищем, он

не хотел выглядеть перед сообществом так, будто потерял над ним контроль. Муларски пояснил, что это не окажется проблемой, поскольку Мастер Сплинтер будет секретным администратором. Никто, кроме них двоих, не узнает, что сайтом теперь управляет новый человек. Для всех остальных Сплинтер так и останется обыкновенным модератором.

«Чувак,» — ответил JiLsi, — «готовь свой сервер. Мы переезжаем.»

Муларски сразу занялся делом. Он арендовал сервер у компании "Планета", базирующейся в Техасе, а затем занялся более темными делами, купив у русского под ником Квазатрон защиту о DDoS за 500 долларов в месяц. Оплата была произведена в электронной валюте. Квазатрон сконфигурировал сайт так, что его публичная часть находилась у Staminus, хостинговой компании с широким каналом и устойчивостью к подобным атакам. Их системы могли выдержать такой поток, а ПО Квазатрона направляло только нужный траффик на настоящий сервер DarkMarket за кулисами.

Все было сделано так, как сделал бы восточно-европейский хакер. Когда Муларски хотел получить доступ к бэкэнду сайта, он использовал KIRE, виргинскую компанию, дававшую «аккаунты-раковины», позволяющие пользователям IRC соединяться с чат-комнатами, не открывая домашнего IP. Никто не узнает, что польский спам-король заходит на сайт из Питтсбурга.

Как только этот ход был сделан, Муларски пошел в суд, и получил ордер на обыск собственного сервера, что позволило ему видеть все базы пользователей, логи доступа и личные сообщения.

Оставалось последнее. После Shadowcrew, обычным делом для кардерских форумов было заставлять принимать пользователей соглашение, по которому на сайте была запрещена всякая незаконная информация, и снимавшее всякую ответственность с организаторов за нее. Хозяева форумов были уверены, что запутанный язык закона сможет их защитить. DarkMarket имел особенно длинное и детальное пользовательское соглашение, так что никто и не заметил, что Мастер Сплинтер добавил строчку.

«Используя этот форум, вы соглашаетесь, что администрация может читать личную переписку на форуме, чтобы убедиться в выполнении соглашения,» — написал он, — «или еще с какой-либо целью».

«Думаю, важно отметить, что Айсмен довольно бестолково мечтает стать хакером, и взламывает сайты просто для удовольствия.»

El Mariachi хорошо знал, за какие ниточки дергать Айсмена. После этого

коварного захвата, уже Дейв Томас вернулся в блог «Жизнь на дороге», чтобы беспрестанно оскорблять своего противника, называя его «Айсбой», «Офицер Айс», и «чертовым куском говна на своих ботинках». Он призывал Айсмена встретиться с ним лично и решить спор по-мужски. Затем он сказал, что мог бы нанять киллера, чтобы тот выслеживал кардера до конца жизни.

Макс отвечал со все возрастающей яростью. Он не забыл трудности и расходы, которые на него свалились, когда он искал новый хост, после того, как Томас отключил его во Флориде. Агрессия, которую он сдерживал в себе с тех самых пор, изрыгалась из его чрева и изливалась через кончики его пальцев. «Ты молокосос, безвольный мешок дерьма. Я мог бы порвать тебя к чертям голыми руками, но трус вроде тебя сразу позовет копов и полезет за оружием, только завидев меня. Лучше молись, чтобы я никогда никуда не выходил, ибо при встрече ты будешь выглядеть еще большим болваном чем сейчас, а я не буду иметь не малейших угрызений совести и сверну тебе шею.»

Успокоившись, он отправил Томасу письмо. Он думал о том, чтобы отключить Рынок Кардеров, и оставить свою личину Айсмена. Нет, это не значило бы, что он сдается, это, напротив, оказалось бы самой серьезной угрозой для кампании Томаса.

> Ты не читал «Искусство войны», идиот? Ты НИЧЕГО про меня не знаешь. Я знаю о тебе ВСЕ.
>
> Я убью Рынок Кардеров, я убью Айсмена, и что тебе останется? Бой с тенью? Ты безнадежен… Я враг, который будет постоянно тебя одолевать, поскольку у тебя НЕТ ЗАЩИТЫ, и НЕТ ЦЕЛИ.
>
> Я твой самый большой ночной кошмар, ты со своей семьей будешь страдать за те деньги, которые я из-за тебя потерял, и очень и очень долго.

Через два дня Макс показал, был серьезен. Он взломал сайт El Marianchi, «The Gifters», который Томас превратил в полулегальный сайт для наблюдения за кардерскими форумами. Он очистил весь жесткий диск… Сайт никогда не поднялся вновь.

Айсмен провозгласил свой триумф в финальном сообщении в блоге. «Мне нечего доказывать. Теперь, повергнув доносчика федералов Дэвида Томаса, я вас покидаю.», написал он. «В отличие от вас, я занимаюсь своим бизнесом. Выучите урок. Идите дальше и оставьте это все.»

Но Максу не дали уйти обратно в тень. Два репортера из «USA Today»

обнаружили публичную войну кардеров и получили подтверждение враждебных захватов от фирм, наблюдавших за форумами. На утро после того, как Макс провозгласил победу над El Mariachi, служба доставки развозила два миллиона экземпляров газеты за четверг по всей стране. На первой странице бизнес-раздела красовалась история о захвате Айсменом кардерских сайтов.

Потворствуя своему эго и вступая в публичную конфронтацию с Девидом Томасом, Макс вывел Айсмена на страницы крупнейшей ежедневной газеты в Штатах.

«Секретная служба и ФБР отказываются давать комментарии по поводу действий Айсмена», заявлялось в статье. «Однако даже так действия этой загадочной личности иллюстрируют растущую угрозу киберпреступности, которая в большой мере является плодом существования некоторых форумов.»

Статья не была сюрпризом, репортеры связались с Айсменом, и Макс отправил им длинный комментарий, выражавших его позицию. Его мнение не было напечатано, и статья лишь сделала Макса еще более дерзким. Он даже добавил цитату из нее в шапку страницы входа на Рынок Кардеров: «Он создал Вол-Март подполья».

Макс показал статью Черити. «Кажется, я поднял изрядную волну».

Крис был в бешенстве, когда узнал про общение Макса с журналистами. Он наблюдал, как Макс тратил бесчисленные часы на пререкания с Томасом, а теперь он еще и давал интервью?!

«Ты потерял всякий рассудок», — заметил он.

Макса затянуло. Заявки в Рынок Кардеров лились рекой. Статья, казалось, заставила всех уличных хулиганов понадеяться на успех в этой области. Сайт принял триста новых обитателей за ночь. Через две недели они все еще прибывали.

Он скинул большую часть обязанностей на администраторов. Было чем заняться помимо этого. Стремительная атака против финансовых организаций была весьма успешна, но файерволы банков оказались самой легкой частью. Банк Америки и Кэпитал Уан, в особенности, были огромными организациями, и Макс попросту заблудился в их обширных сетях. Он легко мог потратить годы на любой из них просто в поисках нужных ему для серьезного результата данных. У Макса были серьезные проблемы с мотивацией для этой отупляющей работы: взлом сетей был весельем, а сейчас он закончился.

Вместо этого, Макс отложил вопрос с банками, сосредоточившись на войне

кардеров… Новый хостинг-провайдер Макса получал постоянные жалобы на преступную деятельность на Рынке Кардеров. Макс видел одно из писем, отправленное с анонимного аккаунта. По наитию, он попробовал войти туда с помощью данных JiLsi. И вдруг, все подошло. Это означало, что JiLsi пытается уничтожить Макса.

Тот затем занялся тем, что вломился в аккаунт JiLsi на русском форуме Mazafaka и отправил лавину сообщений с простым содержанием: «Я федерал». Затем Макс публично продемонстрировал эти доказательства злодеяний JiLsi. Доносы в хостинг компанию, с его точки зрения, были весьма подлой тактикой.

DarkMarket не оказался настолько вежлив, чтобы сразу умереть. Макс мог бы просто уронить базу данных, но это бы не особо сработало — сайт возрождался прежде… Его DDoS атаки перестали быть эффективными. DarkMarket перешел к дорогому широкополосному хостеру, и создал выделенные сервера для почты и баз данных. Внезапно, этот сайт оказался крепким орешком.

Затем, до Макса дошли весьма интригующие слухи про DarkMarket.

История включала в себя Silo, канадского хакера, известного своей удивительной способностью жонглировать дюжиной личин в сообществе, непринужденно меняя стиль под каждую из них. Вторым знаменитым навыком Silo было то, что он был одержим взломом других кардеров. Он постоянно публиковал ПО со скрытым кодом, позволявшее шпионить за коллегами.

Эти две черты сыграли Silo на руку, когда он зарегистрировался на DarkMarket под новой личиной и опубликовал ПО для взлома на оценку. Будучи верным себе, Silo спрятал в программе функцию, отправляющую пользовательские файлы на один из его серверов.

Взглянув на результаты, он обнаружил небольшой кэш пустых шаблонов Ворда, включавший форму жалобы на вирус. Шаблоны содержали логотип организации, известной, как Национальный альянс киберкриминалистики в Питтсбурге. Макс проверил их. Федералы. Кто-то из DarkMarket работал на правительство.

Готовый к расследованию, Макс снова воспользовался бэкдором. На этот раз он шел на разведку. Он вошел в консоль от рута, вывел недавнюю историю входа. Затем он вывел весь этот список в отдельное окно и начал проверять публичные записи о регистрации для каждого IP, использованного администрацией. Дойдя до Мастера Сплинтера, он остановился. Представившийся поляком спамер входил с адреса, принадлежавшего корпорации в США под названием Pembrooke Associates.

Он проверил записи о регистрации на Whois.net для сайта компании

Pembetal.com. Их почтовый ящик находился вВаррендейле, Пеннсильвания, в двадцати милях от Питтсбург. Еще там был номер телефона.

Еще один щелчок мыши, еще одно окно браузера с обратным телефонным справочником на Anywho.com Он ввел номер телефона и получил настоящий адрес: 2000, Технологический проезд, Питтсбург, Пеннсильвания.

Это был тот самый адрес, который относился у Национальному альянсу киберкриминалистики. Мастер Сплинтер был федералом.

Глава 28. «Суд кардеров»

Кейт Муларски был изможден.

Сначала он переговорил с агентом в филиале Секретной службы на другом конце города. «Мне кажется тебе грозят некоторые неприятности». Один из бесчисленных информаторов слышал, что Iceman обнаружил неопровержимые доказательства, что Мастер Сплинтр был либо стукачом, шпионом корпоративной безопасности, либо федеральным агентом. Iceman временно объединился со своим бывшим врагом Silo и готовил подробную презентацию для руководства Carders Market и Dark Market‘a. Iceman и Silo явно хотели засудить Мастера Сплинтра.

Все началось с кода Silo. Известность Мастера Сплинтра как спамера и программиста сделала его специалистом в области обзоров вредоносного кода DarkMarket‘a. Это было одним из преимуществ его тайной операции: Муларски сможет оценить последние версии секретного атакующего кода и передать их CERT, который, в свою очередь, отправит их всем антивирусным компаниям. Вредоносный код можно будет обнаружить еще до того, как он окажется на черном рынке.

В этот раз Муларски поручил код в качестве тренировочного задания одному из студентов CMU проходящих стажировку в NCFTA. Согласно стандартной процедуре студент запустил программу в изолированном режиме на виртуальной машине - своего рода программная чаша Петри, которую после можно вычистить. Но он забыл о флешке в USB-порте. На нее были загружены пустая отчетная форма о вредоносной программе с логотипом NCFTA и основные цели исследования. Прежде чем студент осознал, что произошло, документ оказался в руках Silo.

Шесть администраторов и модераторов DarkMarket получили копию кода Silo. Теперь канадцы знали, что один из них был федеральным агентом.

Silo был темной лошадкой. В реальной жизни он был Ллойдом Лиске, менеджером в автомагазине Ванкувера и фальсификатором кредитных карт, разоренным через несколько месяцев после операции Firewall. Когда он был приговорен к восемнадцати месяцам домашнего ареста, Лиске изменил свою фамилию с Buckell и прозвище с Canucka и вновь появился на сцене кардеров.

Теперь канадец был неприкасаем. В кругах правоохранительных органов было хорошо известно, что Silo был осведомителем полицейского департамента Ванкувера. Вот почему он всегда взламывал других хакеров: троянский конь,

проникший в NCFTA, не собирался разоблачать операции правоохранительных органов, Silo просто пытался собрать сведения на членов DarkMarket‘a для полиции.

Silo не был слишком верен ФБР, но скорее всего не собирался из кожи вот лезть, чтобы раскрыть тайную операцию бюро. К несчастью, Iceman узнал о разведке и организовал рейд по сбору информации на DarkMarket. Именно в этот момент неосторожность Муларски сделала свое дело. Он как обычно зашел в DarkMarket с помощью оболочки KIRE, скрывающей его местоположение. Но JiLsi как требовательный начальник постоянно напрягал Мастера Сплинтра задачами по обслуживанию - например, загрузкой новых рекламных баннеров - задачи, требующие немедленного выполнения. Иногда в это время KIRE бездействовал, и он по ссылке заходил напрямую. Iceman поймал его.

Даже тогда, он должен был быть в относительной безопасности. Офис по оказанию широкополосных услуг был создан под видом фиктивной корпорации, с телефоном, звонившим по непрослушиваемому VoIP в комнату связи. Телефонная линия не должна была засечься. Так или иначе, этого не произошло, и Iceman получил адрес и определил, что он принадлежит NCFTA.

Муларски быстро отправился в комнату связи, провел картой доступа, и заперся внутри. Он установил канал для безопасной связи с Вашингтоном. Агент не приукрасил свой отчет руководству. Несмотря на его работу над получением тайной власти для контроля DarkMarket‘a, при поддержке от главного Управления Юстиции и должностных лиц бюро, Iceman собирался разнести их в пух и прах всего через три недели после начала работы.

Макс боролся над предотвращением обнаружения - он знал, что после его атаки DarkMarket‘a, все его данные будут использованы против него. Он рассматривал вариант закрытия Carders Market до разоблачения Мастера Сплинтра, как возможность избежать того, что бы это все было воспринято просто еще одним залпом в войне кардеров. Вместо этого, он решил отправить своего нового лейтенанта, Th3C0rrupted0ne, чтобы представить свою позицию.

Суд задерживала «Carder IM» Silo - бесплатная, якобы зашифрованная программа для обмена бесплатными сообщениями, которую канадский хакер предложил в качестве альтернативы AIM и ICQ, поддерживающий показ объявлений для поставщиков дампов. Matrix001 обнаружился со стороны DarkMarket‘a - JiLsi был занят с последствиями от нападения Макса на Mazafaka. Также присутствовали Silo с другими двумя канадцами. Silo открыл заседание, раздав архив RAR с доказательствами, собранными им и Iceman‘ом.

Когда некоторые из кардеров открыли файл, их антивирусы обезумели. У Silo

оставил бэкдор в доказательствах; не самое многообещающее начало встречи на высшем уровне.

C0rrupted и Silo продолжали представлять доказательства: шаблоны документов Silo показало, что кто-то в NCFTA получил привилегированное положение на Darkmarket, а логи доступа, украденные Iceman'ом доказывали, что Мистер Сплинтр был кротом.

«Неоспоримое доказательство», написал C0rrupted. «Мы упорно работали, пытаясь заключить мир, и если это станет достоянием общественности, органы правопорядка будут преследовать нас по пятам. Однако, если мы ничего не сообщим, мы будем ответственны за всех тех, кого наебут.»

«Все это действительно так», сказал Silo.

Это не убедило Matrix'а. Он запустил собственный Whois на доменное имя Pembrooke Associates и с помощью Domains by Proxy получил только анонимный список: в нем не было адресов и телефонных номеров. «Бля», напечатал Matrix. «Вы даже не проверили информацию и компании, полученные из Whois, не так ли? Кто передал вам эти материалы?»

«Это не мои материалы,» написал Silo. «Они Iceman'а».

«Так вы верите любому присланному вам дерьму? Даже не проверив его?»

Свидетельства, предоставленные Silo больше не убеждали Matrix'а: В шаблонах NCFTA были структурные и орфографические ошибки - как ФБР или некоммерческая организация безопасности могла сделать настолько дрянную работу? Кроме того, было хорошо известно презрение Iceman к Darkmarket'у, да и Silo был вечной занозой.

Обстановка накалялась. C0rrupted отключился, а остальные умолкли, когда Silo и Matrix начали перекидываться оскорблениями. «У тебя есть хоть что-то, что заставит меня поверить тебе?» спросил Matrix.

«Не надо», наконец ответил Silo. «Не надо верить мне. Свали из моей IM … Отправляйся за решетку.»

Муларски был исключен из чата, но, когда оно закончилось, Matrix передал логи Мастеру Сплинтру. Агент был рад что в последнюю секунду он успел вычистить всю информацию: как только он узнал об Iceman'овским планах его разоблачения, он связался с регистратором доменных имен и заставил компанию удалить всех людей связанных с Pembrooke Associates и их телефонные номера из своих реестров. Потом он запросил Anywho вывести листинг его секретной телефонной

линии. Эта чистка непременно убедит Iceman‘а, что Мастер Сплинтр - федерал, но больше никто не сможет проверить истинность его выводов.

Теперь Муларски начал убеждение по ICQ. Он сказал Matrix‘у и всем, кто слушал, что он невиновен. Он обратил внимание кардеров на логи, выделяя все случаи, когда он заходил в систему с IP-адреса KIRE. Это мои входы в систему, писал он. Я не знаю, чьи остальные.

Затем он развернулся и атаковал. Сомнения Iceman‘а в JiLsi работали в его пользу. Все пошло наперекосяк, он написал. JiLsi вел себя подозрительно. С одной стороны, он поручил Мастеру Сплинтру никому не говорить, сервер уже запущен. С другой - JiLsi создал впечатление, что DarkMarket находится в стране, недоступной для западных правоохранительных органов, хотя на самом деле располагался в городе Тампа, штат Флорида, где копы могли с легкостью раздобыть ордер на обыск. Это действительно было странно.

JiLsi твердил о своей невиновности, но вел себя слишком странно для этого. Мастер Сплинтр публично поблагодарил Iceman‘а, за то, что тот довел дело до его сведения и сказал, что он сразу выведет DarkMarket за пределы Соединенных Штатов.

Муларски связался с правоохранительными органами Украины, и они помогли ему быстро получить там хостинг. В мгновение ока, Darkmarket оказался в Восточной Европе. Большинству кардеров пришлось согласиться, что федералам не удастся провести свою операцию в бывшей советской республике.

Формальный вердикт не был озвучен, но единогласным решением была определена невиновность Мастера Сплинтра. Но они не были столь уверены в JiLsi.

Когда споры утихли, Муларски вернулся к своей обычной тайной операции. Несколько недель спустя, когда он писал отчеты, его вызвал другой агент.

Специальный агент Майкл Шулер был легендой среди агентов киберпреступлений Бюро. Именно он взломал компьютеры русских во время операции Invita. Сейчас, работая в Ричмонде, штат Вирджиния, в качестве полевого офицера, Шулер сообщал о нарушении в соседнем Capital One. Служба безопасности банка обнаружила атаку с использованием уязвимости в Internet Explorer. Они прислали Шулеру копию кода, и он хотел, чтобы Муларски поручил одному из гиков NCFTA поработать с ним.

Муларски слушал, как Шулер описывал свое расследование на сегодняшний день. Он сосредоточился на фейковом сайте новостей, Financialedge.news.com, используемом для распространения вредоносных программ. Домен был

зарегистрирован на подставное лицо в Грузии. Но когда регистратор Go Daddy, проверил свои записи, он нашел, что тот же пользователь уже регистрировал другой адрес с помощью их компании.

Cardersmarket.com

Муларски сразу понял всю важность этого. Iceman представлял себя как невиновного владельца сайта, на котором произошло обсуждение незаконных действий. Теперь у Шулера были доказательства, что он также был жадным до денег хакером, проникшим сеть пятого по величине эмитента кредитных карт Америки. «Чувак, у тебя дело!» рассмеялся Муларски. «Ты только что получил дело по парню, которого выслеживает наша Group II. Нам нужно работать над этим вместе.»

На другом конце города, агенты Секретной службы в местном отделении Питтсбурга независимо тоже сделали открытие об Iceman‘е: информатор передал конфиденциальную информацию, что главный руководитель Carders Market также известен как поставщик дампов Digits. Через четыре дня после статьи в USA Today, агенты вытянули эту информацию благодаря второму кроту, который совершил контролируемую закупку у Digits: двадцать три дампа по $480 в e-gold.

Этого было более, чем достаточно, для обвинения в уголовном преступлении.

Глава 29. «Одна Платиновая и шесть Классических»

Кейт Муларски не осознавал что делает, когда взял на себя DarkMarket.

Его дни стали настоящим безумием. Каждый день начинался в 8 утра с проверки ICQ сообщений свалившихся за ночь на предмет какой-либо работы для MasterSplinter‘а. Он отправлялся на DarkMarket - сайт функционировал. Наткнуться здесь на Iceman‘а было всегда крайне тяжело.

Затем настала очередь нудной работы по резервному копированию БД. Iceman дважды сбрасывал таблицы в тщетных попытках вывести Mularski на чистую воду, так что теперь возня с бэкапами была частью утренней рутины. Нельзя было забывать о расследовании: пока база продолжала копироваться, простой скрипт, автором которого был программист NCFTA, сканировал каждую строку на предмет 16-ти значных чисел, начинающиеся с цифр 3 по 6. Украденные кредитки автоматически сортировались по BIN и отправлялись соответствующим банкам для немедленного аннулирования.

Затем Mularski бегло просмотрел приватные месседжи, отобрал наиболее интересные чаты и проверил их в ФБР-овской центральной базе данных электронного наблюдения под названием ELSUR. Следующие несколько часов были потрачены на написание отчёта. Под ником Master Splinter, Mularski начал обналичивать средства на скромные суммы. Некоторые банки согласились поспособствовать и поделились имеющимися дампами с фейковыми именами, но реальными транзакциями, обработка которых финансировалась уже из бюджета ФБР.Он передал им список с номерами PIN кардеров по всей стране, финансовые учреждения в свою очередь ежедневно докладывали о том где и когда осуществлялся вывод средств. Mularski передавал информацию местным агентам в зависимости от города, где совершались операции, что приводило к регулярному написанию детальных заметок.

В три часа, когда кардеры начинали появляться в сети, «вторая» жизнь Mularski превращалась в пекло. Каждый пытался что-нибудь узнать у «Сплинтера». Были разные темы, например как завалить вендора, который кидает заказчиков, жалобами или как грамотно предъявить обвинения. Парни обращались к нему за бесплатными дампами или за спам услугами.

Муларски возвращался домой к концу дня, только для того, чтобы снова залогиниться. Для правдоподобности, «Сплинтер» должен был работать в те же часы, что и реальные кардеры. Так проходил каждый вечер - домашний диван, телик, включенный на случайный канал и открытый бук. Он был онлайн в DarkMarket-е, AIM, ICQ - отвечал на вопросы, назначал рецензентов, утверждал вендоров и банил рипперов. В онлайн он был обычно до двух ночи, взаимодействуя с подпольем.

Для выполнения поставленных целей, нужно было втереться в доверие. Он раздавал «подарки», которые якобы были оплачены с украденных кредиток, но на самом деле, оплачивались из средств бюро. Cha0, турецкий криминальный авторитет и администратор DarkMarket-а желал легковесный комп, который продавался в штатах. Муларски отправил два таких ПК на сброшенный от Cha0 адрес в Турции. Играя в Санту нужно было следовать правилам: оставаться под прикрытием, создавая видимость зарабатывания денег не задавая лишних вопросов.

Для себя он отметил, что быть боссом в мире киберкрайма, достаточно тяжёлая работа. Во время путешествий или отпуска, он должен был хотя бы вкратце предоставить причину своего отсутствия на форуме, чтобы не вызвать подозрений. В январе 2007-ого он заранее дал знать, что будет в полёте некоторое время, но не сказал куда и зачем летит. Он собирался в Германию, чтобы обсудить с прокурорами Matrix001, соучредителя DatkMarket‘a.

Кроме всего прочего, Matrix001 был первоклассным спецом в своём деле и вообще мастером на все руки. Он создавал и продавал фотошоповские шаблоны, прибегая к помощи «специалистов» по изготовлению фальшивых кредиток или фейковых ID. Он мог предоставить такие шаблоны, как: Visa, MasterCard, American Express, U.S. карту социальной защищённости, печати нотариусов и водительские права действующие в северных штатах. Так например, шаблон Американского паспорта он продавал по 45$, а карту Visa 125$.

Отношения между «Сплинтером» и Matrix001 значительно улучшились за последние три месяца: Муларски и немец любили видео-игры и болтали о них целыми ночами. Также они общались и о делах - тогда немец поделился тем, что недавно получил денежные переводы от своих продаж из города Eislingen который находится в Южной Германии. Это можно было назвать первой зацепкой в разоблачении всей цепочки.

Здесь решался вопрос следования денег. Как и все кардеры, Matrix001 предпочитал проводить оплаты посредством e-gold — платёжное средство для безналичных платежей через Интернет.), электронной платежной системы, созданной бывшим онкологом по имени Дуглас Джексон в 1996. В противовес

PayPal, e-gold была первой виртуальной валютой подкреплённой слитками серебра и золота, которые хранились в банковских сейфах Лондона и Дубаи.

Это была мечта Джексона - запилить первоклассную международную систему без всякой привязки к правительству. Преступникам он нравился. В отличие от реального банка, E-gold не применял никаких средств валидации пользователей; так зачастую в профилях фигурировали такие имена как «Mickey Mouse» и «No Name». Чтобы положить или обналичить деньги в E-gold, пользователи могли воспользоваться любым из сотни обменников по всему миру, которые могли осуществлять как простые денежные переводы, так и анонимные; помимо всего прочего, они также могли принять наличные и конвертировать её в E-gold (если сумма не покрывала полные слиток, то он мог подлежать «кройке»). Обменники также занимались конвертацией из виртуальных средств в местную валюту, которую можно было получить через Western Union, PayPal или банковский перевод. Одна компания даже предложила «G-карты» с предустановленным ATM чипом - это позволило бы владельцем E-Gold вывести средства через любой банкомат.

Очевидно что E-Gold был для преступников «хлебом и маслом». К декабрю 2005-ого года было установлено, что более 3000 счетов фигурировали в «кардинге», ещё 3000 использовались для покупки и продажи детского порно и 13000 счетов были задействованы в инвестиционных аферах. Их было достаточно легко обнаружить: так например в операция связанных с детским порно, в примечаниях к операции можно было наблюдать имена, например «Lolita», в Ponzi схемах «HYIP» («High-Yield Investment Program» - «Высоко-Доходная Инвестиционная Программа»). Кардеры включали своего рода метки того, что они покупали: «For 3 IDs»; «for dumps»; «10 classics»; «Fame’s dumps»; «10 M/C»; «one plat and six classics»; «20 vclassics»; «18 ssns»; «10 AZIDs»; «4 v classics»; «four cvv2s»; «for 150 classics».

В течении долгого времени, E-Gold закрывала глаза на криминальные сделки. Их сотрудники конечно блокировали некоторые профили связанные с детским порно, но ничего не могли поделать с тем, что злоумышленники всё равно могли вывести деньги со счёта. Но отношение компании резко изменилось, после того агенты ФБР и Секретных служб, получив ордер, провели проверку в офисах E-Gold в Мельбурне и Флориде, после чего выдвинули обвинение против Джексона за предоставление услуг денежных переводов без лицензии.

Джексон начал добровольно исследовать имеющуюся базу на предмет преступных операций и отправлял «зацепки» в U.S. Postal Inspection Service - единственное агентство, которые не пыталось упечь его в тюрьму.

Его становление «на путь истинный» было как нельзя кстати для Муларски.

Благодаря Грегу Краббу и его команде в почтовом отделении, Муларски запросил у Джексона информацию о профилях Matrix001, который был зарегистрирован под псевдонимом «Ling Ching».

Когда Джексон просматривал базу, то обнаружил что эта запись, первоначально была создана под другим именем: Markus Kellerer, а в качестве адреса был указан город Айзлинген в Германии. В ноябре Муларски направил официальный запрос о по данному человеку в представительство Немецкой Национальной Полиции через консульство США во Франкфурте. Германия подтвердила - Kellerer был реальным человеком, а не ещё одним псевдонимом, после чего Муларски забронировал место на рейс в Штутгарт.

Matrix001 был первой фигурой из братства DarkMarket, кого удалось арестовать. Муларски несомненно хотелось бы найти ещё кого-нибудь, кто был не прочь потрепаться о видеоиграх.

• • •

Вернувшись из Питтсбурга, он вновь окунулся в работу, взявшись за легенду Iceman. Он искал любое упоминание об Iceman‘е - был некто с таким ником на Shadowcrew и ещё несколько упоминаний о нём в IRC чатах. Они всегда пытались пустить по ложному следу. Теперь Муларски прорабатывал идею о том, что Iceman-а не существует.

Должно быть Iceman сотрудничал с Канадским информатором Ллойдом «Silo» Лиске - это было интересно. Silo работал с Iceman‘ом пытаясь вывести Муларски на чистую воду. Это возможно и не имеет особого значения, информаторы часто выкрикивают обвинения, например КОП или СТУКАЧ, чтобы отвести подозрения от себя. Но Silo сказал своим операторам в департаменте полиции Ванкувера, что он взломал комп Iceman-а, и что даже выжав из себя все соки, не сможет узнать его настоящее имя или действительный IP адрес. В результате оказалось что «Silo» имел множество E-Gold аккаунтов, один из которых был под именем «Keyser Söze».

Если Лиске был фанатом фильма «Подозрительные лица», возможно, он мог примерить на себя шкуру криминального кардинала и кормить правоохранительные органы всякой чепухой, касательно подозрительных фигур в криминальном мире, пользуясь своим служебным положением.

Муларски вылетел в Вашингтон, где представил свою теорию для Секретных служб в их штаб-квартире, но потерпел фиаско. Дело в том, что Секретный департамент тесно сотрудничал с Департаментом полиции Ванкувера и считали Silo хорошим парнем.

Секретная служба пустила по ложному следу сама себя. В лаборатории головного офиса в Питтсбурге, агенты выводили схемы состоящие из имён соединённых между собой линиями. Многие имена уже были вычеркнуты. Это была их собственная, постоянно меняющаяся дорога к Iceman-у и его миру.

Муларски вернулся в Питтсбург и оба агентства возобновили поиски такой персоны киберпространства как Keyser Söze - «безнаказанно» хакнувшего Iceman-a.

Глава 30. «Максик»

Макс мог видеть, что происходило. С агентом ФБР у руля, DarkMarket шел к тому, чтобы упрятать многих кардеров за решетку. Но, как Кассандра из Греческой мифологии, он был проклят знать будущее, и чтобы никто ему не верил.

Между статьей USA Today и его провалившейся попыткой разоблачить Master Splyntr, Макс чувствовал, как напряг давит на него. В ноябре он заявил об уходе Iceman'а и устроил шоу с передачей сайта под контроль Th3C0rrupted0ne.

Изолировал самого себя от общества пока обстановка не успокоилась и через три недели забрал доску объявлений обратно уже под другим псевдонимом. Iceman умер; да здравствует «Aphex».

Макс устал от тесного жилища в Post Street Towers, потому Крис перетащил Нэнси, одну из его обнальщиц, в Сан Франциско, чтобы снять для Макса однокомнатную в Archstone'овском возвышающемся комплексе корпоративных апартаментов Fox Plaza в деловом районе. Она была поставлена в качестве торгового представителя в Capital Solutions, корпорации напротив Aragon, используемой для отмывания части его прибыли. Ти, вернувшись из поездки в Монголию, получила задание быть в квартире и принять доставку кровати, оплаченной с ее легальной карты American Express. Крис позже рассчитался с ней.

К январю 2007 Макс вернулся к делам в своем новом убежище с кучей WiFi, развернутых вокруг. Fox Plaza был гигантским шагом к роскоши по сравнению с Post Street Towers, но Макс мог это себе позволить – он мог оплатить месячную ренту всего после пары успешных дней торговли дампами. Как и Digits, Макс теперь был признан некоторыми кардерами как второй наиболее успешный продавец магнитных полос в мире.

Первое место в списке было прочно занято украинцем, известным как Maksik. Maksik работал вне кардерских форумов, запустив свой собственный веб-магазин краденых карт на Maksik.cc. Покупатели должны были сначала отправить Maksik предоплату через e-gold, WebMoney, почтовым переводом или через Western Union. Таким образом, они покупали доступ к его веб-сайту, где они могли уже выбирать дампы, которые хотели по BIN'у и типу карты и месту оформления. Со своей стороны Maksik нажимал кнопку, чтобы подтвердить транзакцию, и покупатель получил бы электронное письмо с дампами, которые он заказал, прямо из Maksik'овской огромной базы данных похищенных карт.

Изделия от Maksik'а были феноменальны, с высоким процентом успеха на кассе и с громадной выборкой BIN'ов. Как и у Макса, карты Maksik'а были получены при проведении их в PoSтерминалах торговых точек. Но вместо набивания очков на маленьких магазинчиках и ресторанах, Maksik получал его карты из гораздо меньшего числа гигантских целей: Polo Ralph Lauren в 2004; Office Max в 2005. В течении трех месяцев, Discount Shoe Warehouse потерял 1.4 миллиона карт, полученных из 108 магазинов в 25 штатах, попавших прямо в базу данных Maksik'а. В июле 2005, рекордное число в 45.6 миллионов дампов были украдены из принадлежащей TJX торговой сети T. J. Maxx, Marshalls, и HomeGoods.

Это было то время, когда подобные утечки могли оставаться в секрете между хакерами, компаниями, и федеральными правоохранительными органами, а пострадавшие клиенты держались в неведении. Чтобы подтолкнуть компании сообщать об утечках, некоторые агенты ФБР следовали негласному принципу убирать имена компаний из обвинительных актов и пресс–релизов, защищая корпорации от плохой рекламы в виду их ничтожной безопасности. В случае 1997 года с Карлосом Сальгадо младшим – первая крупномасштабная онлайн кража кредитных карт – власти убедили судью, выносящего приговор, навсегда опечатать судебный протокол, из-за страха, что пострадавшую компанию ждет «потеря бизнеса в виду сложившегося мнения, что компьютерные системы могут быть уязвимы.» Следовательно, восемьдесят тысяч жертв никогда не были уведомлены, что их имена, адреса и номера кредитных карт были выставлены на продажу в IRC.

В 2003 году штат Калифорния эффективно прекратил подобные сокрытия, когда законодательной властью был принят SB1386, первый национальный закон об обязательном раскрытии утечек. Закон обязывал взломанные хакерами организации, которые вели бизнес в Золотом Штате, оперативно предупреждать потенциальных жертв кражи личных данных об обнаруженной утечке. В последующие годы сорок пять других штатов приняли подобные законы. Теперь ни одна значительная утечка данных о покупателях не оставалась в секрете надолго, с момента обнаружения компанией и банками.

Заголовки вокруг брешей в гигантских магазинах только добавили блеска Maksik'ому продукту – он не пытался скрыть тот факт, что торговал дампами из торговых сетей. Когда атака на TJX появилась в новостях в январе 2007 года, детали, которые были обнародованы, также подтвердили то, о чем многие кардеры уже подозревали: у украинца был хакер в США, снабжающий его дампами. Maksik был посредником таинственного хакера из штатов.

В середине 2006 года хакер, по всей видимости, был в Майами, где он запарковался у двух магазинов Marshalls, принадлежащих TJX, и взломал их WiFi. Отсюда он прыгнул в локальную сеть и пробился к штаб-квартире корпорации, где

он запустил пакетный сниффер, чтобы поймать вживую транзакции кредитных карт из магазинов Marshalls, T. J. Maxx, и HomeGoods по всей стране. Сниффер, как будет позже обнаружено расследованием, работал незамеченным семь месяцев.

У Макса был соперник в Америке, и чертовски хороший.

Благодаря в большей степени хакеру Maksik'а и Max Vision'у, популярное мнение среди потребителей, что веб-транзакции были более безопасны, чем покупки в реальной жизни, теперь стало полностью ошибочно. В 2007 году большинство скомпрометированных карт были украдены из розничных магазинов и ресторанов. Проникновения в огромные магазины приводили к компрометации миллионов карт за раз, но дыры в маленьких точках продаж были более распространены – анализ Visa обнаружил, что 83 процента утечек кредитных карт были из магазинов, обрабатывающих миллион или меньше Visa транзакций в год, при этом большинство краж происходило в ресторанах.

Макс пытался удержать источники его дампов в секрете, ложно утверждая в постах на форуме, что данные получены из центров обработки кредитных карт, чтобы сбить следователей с пути. Но Visa знала, что PoSтерминалы в ресторанах были под ударом. В ноябре 2006 года компания выпустила брошюру для индустрии услуг в сфере питания, предупреждающую о хакерских атаках, происходящих через VNC и другие программы удаленного доступа. Макс, не смотря на это, продолжал находить постоянный поток уязвимых закусочных.

Но Максу этого было недостаточно. Он не уходил в бизнес кражи данных, чтобы быть вторым из лучших. Maksik стоил ему денег. Даже Крис теперь покупал у двоих: у Макса, и у Maksik'а, в зависимости от того, какой продавец предложит ему выгодную сделку с лучшими дампами.

По указанию Макса, Ти в течении нескольких месяцев подружилась с украинцем и убеждала его начать торговлю на Carders Market'е. Maksik вежливо отказал и предложил посетить его когда-нибудь в Украине. Получив отказ, Макс сбросил перчатки и дал Ти троянскую программу для отправки Maksik'у, надеясь получить контроль над базой дампов украинца. Maksik высмеял попытку взлома.

Возможно, Максу было бы комфортней, если бы знал, что не он единственный был разочарован серьезной безопасностью Maksik'а.

Федеральные правоохранительные органы отслеживали Maksik'а с того момента, как он стал самым влиятельным преступником в результате «Операции Фаервол». Агент Секретной Службы, работая под прикрытием, покупал у него дампы. Почтовый инспектор Грег Крэбб работал с правоохранительными органами в Европе для поимки кардеров, которые вели дела с Maksik'ом, и теперь он

предоставил полученную информацию Украинской национальной полиции. В начале 2006 года украинцы окончательно установили, что Maksik – это некто Максим Ястремский из Харькова. Но у них не было достаточных доказательств для ареста.

Соединенные Штаты перефокусировались на вычислении источника взломов Maksik'a. Egold в который раз предоставил отправную точку. Секретная Служба проанализировала аккаунты Maksik'a в базе данных egold и обнаружила, что с февраля по май 2006 года Maksik перевел $410,750 со своего аккаунта на счет «Segvec», продавца дампов на Mazafaka, предположительно находящегося в Восточной Европе. Исходящий перевод подразумевал, что Segvec – это не один из клиентов Maksik'a, а поставщик, получающий свою долю.

У федералов появился шанс на более точную информацию в июне 2006 года, когда Maksik отдыхал в Дубае. Агенты Секретной Службы из Сан Диего работали с местной полицией для осуществления «подкрадись-и-загляни» в его комнату, где они тайно скопировали его жесткий диск для анализа. Но это был тупик. Важный материал на его диске был зашифрован программой, называющейся Pretty Good Privacy. Этого оказалось вполне достаточно, чтобы остановить Секретную Службу на своем пути.

Кардеры, такие как Maksik и Макс, были на передовой в освоении неожиданного подарка компьютерной революции: криптографические программы сильны настолько, что, в теории, даже НСБ не могла бы их взломать.

В 1990е годы Министерство Юстиции и ФБР Луис Фриха очень пытались сделать подобное шифрование незаконным в Соединенных Штатах, опасаясь, что оно будет освоено организованной преступностью, педофилами, террористами и хакерами. Эти усилия были обречены. Американские математики потратили десятилетия, прежде чем разработать и опубликовать высоконадежные алгоритмы шифрования, которые соперничали с правительственными собственными сертифицированными системами; джин был выпущен из бутылки. В 1991 году программист из США и активист по имени Фил Циммерман выпустил бесплатную программу Pretty Good Privacy, которая была доступна через интернет.

Но это не остановило попытки правоохранительных органов и разведки. В 1993 году администрация Клинтона начала производство так называемого Clipper Chip, разработанного НСБ чипа шифрования, предназначенного для использования в компьютерах и телефонах, спроектированного с функцией «восстановления ключа», которая позволила бы властям взламывать шифр при необходимости на законных основаниях. Чип имел полный провал на рынке и к 1996 году проект умер.

После этого законодатели начали медленно действовать в противоположном направлении, говоря о пересмотре экспортных ограничений эпохи Холодной войны, которые классифицировали сильное шифрование как «вооружение», в основном запрещенное на экспорт. Ограничения заставляли технологические компании убирать сильные шифры из ключевого интернет-софта, ослабляя онлайн безопасность; в то же время, зарубежные компании не были связаны законами и находились в выгодном положении, чтобы опередить Америку на рынке шифрования.

Федералы ответили суровым встречным предложением, которое сделало бы пятилетним уголовным преступлением продажу в Америке любого софта для шифрования без встроенного «черного хода» для правоохранительных органов и тайных агентов властей. В постановлении подкомитета Палаты в 1997 году, юрист из Министерства Юстиции предупредил, что хакеры стали бы основными потребителями законного шифрования, и использовал арест Карлоса Сальгадо в подтверждение своей позиции. Сальгадо зашифровал CDROM, содержащий восемьдесят тысяч номеров украденных кредитных карт. ФБР смогло получить к ним доступ только благодаря тому, что хакер передал ключ подставному покупателю.

«В этот раз нам повезло, так как покупатель Сальгадо работал на ФБР,» – говорилось в официальном заявлении. «Но если бы мы расследовали этот случай по–другому, правоохранительные органы не смогли бы проникнуть к информации на CDROMе Сальгадо. Преступления вроде этого имеют серьезные последствия в части возможностей правоохранительных органов по защите коммерческих данных наряду с неприкосновенностью частной жизни.»

Но федералы проиграли шифровойны и уже к 2005 году невзламываемое шифрование было легко доступно каждому, кто его хотел. Предсказания о гибели в основном не оправдались; большинство преступников не были достаточно технически подкованы, чтобы применять шифрование.

Макс, однако, был. Если бы вся его торговля провалилась и федералы пробились бы сквозь дверь его убежища, они обнаружили бы, что все, что он собрал в ходе преступлений, от номеров кредитных карт, до хакерского кода, зашифровано с помощью сделанной в Израиле программы для шифрования, называемой DriveCrypt – 1,344-битный шифр военного класса, который он приобрел примерно за $60.

Он ожидал, что власти арестовали бы его в любом случае и потребовали бы от него ключевую фразу. Он утверждал бы, что забыл ее. Федеральный судья какого-либо места приказал бы ему раскрыть секретный ключ, и он отказался бы. Он будет под подозрением, может быть год, а затем отпущен. Без его файлов у властей не

будет никаких доказательств о реальных преступлениях, совершенных им. Не оставлено никаких шансов – Макс был уверен. Он был недостижим.

Глава 31. «Суд»

Кардер с Лонг-Айленда Джонатан Джианноне, с которым Макс и Крис познакомились, когда он был тинэйджером, хранил тайну ото всех.

В день, когда Макс своим сайтом поглотил всех конкурентов, агенты Тайной службы арестовали Джианноне в доме его родителей за продажу нескольких дампов Макса Бретту Джонсону, информатору Тайной службы под ником Gollumfun. Джианноне выпустили под залог, но о своем проколе он никому не сказал. Он считал это очередной мелкой неприятностью. В конце концов, ну что ему грозило за продажу двадцати девяти дампов?

Впечатление укрепилось после того, как уже через месяц после ареста суд Южной Каролины снял с него запрет на перемещение. Джианноне тут же полетел в аэропорт Окленда за покупками, где его встретила Ти. Они катались по шоссе вдоль тихоокеанского побережья, она покупала ему пиццу в Fat Slice на Берклиз Телеграф Авеню. Джианноне казался ей забавным - хвастливый белый паренек с вьющимися волосами и пристрастием к хип-хопу, который как-то раз хвалился, что побил футболиста из Нью-Йорк Джетс во время драки в местном баре. Теперь у них появилось что-то общее: Крис прервал контакты с Джианноне незадолго до ареста, а Ти сказал вернуться к заливу Сан-Франциско, чтобы она не создавала проблем в отношениях Криса. Он избавился от них обоих.

Крис позвонил Ти когда они гуляли и очень удивился, когда узнал что Джианноне тоже в городе. Он попросил передать телефон Джанноне. «Таскаешь моих девушек по вечеринкам?» - поинтересовался Крис, злой от того, что Джианноне строит отношения с кем-то из его людей. Это могло серьезно повредить его команде обналички.

«Нет, просто случайно оказался в городе и решил с ней увидеться», - ответил Джианноне.

Это был последний телефонный разговор Джанноне с Крисом. Джанноне отправился домой. Он поддерживал связь с Ти, и несколько месяцев спустя предупредил, что лучше с ним рядом не показываться. Он подозревал, что в поездке к заливу Сан-Франциско за ним следили.

«У меня сейчас проблемы», - сказал Джианноне

«Какие именно?» - спросила Ти. Джианноне нравился такой дух опасности.

«Меня судят на следующей неделе.»

Судебные заседания по делам федерального уголовного права проводятся редко. В надежде хоть немного скостить огромные тюремные сроки, устанавливаемые жесткими нормативными документами, большинство подозреваемых признают вину до суда, а то и вовсе соглашаются на работу информатора. Так было закрыто 86% дел в 2006 году, когда состоялось слушание по делу Джианноне. Ещё в девяти процентах случаев обвинения были сняты с подозреваемых до суда, обычно из-за незначительности дела и риска его проиграть. Как только заседание началось - шанс на оправдательный приговор равнялся примерно одному из десяти.

Джианноне такой расклад устраивал. Далеко не каждое дело опирается на расследование, которое проводил действующий киберпреступник. Бретт «Gollumfun» Джонсон после раскрытия Джианноне уже четвертый месяц проворачивал свою схему с налогами по всей стране, побывав в Техасе, Аризоне, Нью-Мехико, Лас-Вегасе, Калифорнии и Флориде, где его и арестовали в Орландо с рюкзаками набитыми долларами, общей суммой чуть меньше $200 000. Выступать свидетелем со стороны обвинителя он не мог.

Судебный пристав раздал блокноты и ручки двенадцати присяжным, прокурор небрежным тоном начал вступительную речь:

«Я обожаю Интернет», - сказал он. - Интернет - великолепная штука! С его помощью мы можем находить себе развлечения, получать знания, смотреть видео, играть в игры. Можем покупать вещи. Для этого есть eBay, там можно покупать товары, как на аукционе. Там продается всё о чём только можно подумать. Однако, дамы и господа, у Интернета есть другая сторона, о которой мы не любим вспоминать. Тёмная изнанка, где покупают, продают и обменивают не шмотки и побрякушки. Там продают, покупают и обменивают человеческие жизни… Сегодня вы увидите эту сторону Интернета и, уверяю вас, больше не взглянете на Интернет по-старому.

Заседание продолжалось три дня. Прокурор сразу же избавился от Бретта Джонсона, признав Gollumfun‘а лжецом, предавшим своих кураторов из Тайной службы. Потому правительство не допустило его до дачи показаний. В качестве основного «свидетеля» выступали логи чатов Джианноне с информатором, и эти записи говорили сами за себя.

Адвокат Джианноне старался очернить логи. «Машины иногда ошибаются». Он обратил внимание суда на то, что украденные кредитные карты не были использованы в преступных целях и что пострадавших не было. Он напомнил, что от действий его подзащитного никто не умер и не понес физического ущерба.

После одного дня обсуждений суд вынес вердикт: виновен. Так завершилось первое в истории федеральное заседание по делу о кардинговом подполье. Судья потребовал заключить Джианноне.

Неделей позже Джианноне вывели из его камеры в тюрьме Лексингтон Кантри. У выхода из тюрьмы, у двух стальных дверей, отделявших его от свободы, он заметил агентов Тайной службы. Он их узнал - эти двое курировали Джонсона и выступали обвинителями на суде по делу Джианноне.

«Мы хотим знать, кто такой Iceman», - сказал один из них.

«А кто такой Iceman?» - с невинным видом спросил Джианноне.

Агенты дали понять, что положение серьезное. Iceman угрожал убить президента. Джианноне потребовал своего адвоката и агенты тут же ему позвонили. Юрист порекомендовал согласиться на интервью, рассчитывая на снисхождение к своему подзащитному.

Следующие три недели Джианноне постоянно возили из тюрьмы на допросы в тот же самый офис, где Gollumfun планировал операцию по его поимке. В отличие от большинства кардеров, Джианноне не собирался никого выдавать и требовал проведения заседания. Однако теперь его ждало тюремное заключение сроком в пять лет. А ему был всего двадцать один год.

И Джианноне рассказал им всё, что знал: Iceman жил в Сан-Франциско, неплохо торговал дампами карт, иногда продавал товар под псевдонимами Digits и Generous. Чтобы заметать следы - взламывал сети Wi-Fi. Его русским переводчиком была женщина из Монголии по имени Ти. Самое важное - у него был деловой партнер по имени Кристофер Арагон из Орандж Кантри, Калифорния. Вам нужен Iceman? Найдите Криса Арагона.

Эти сведения всполошили всех, кто участвовал в розыске Iceman‘a. Когда Кейт Муларски ввел имя Криса Арагона в систему управления делами ФБР, он нашел отчёт Вернера Джанера за 2006 год, где поставщик дампов для Криса был описан как высокий человек с волосами, забранными в хвост, по имени «Хакер Макс.» Дальше - больше. В декабре 2005 года Джефф Нормингтон был арестован при получении денежного перевода от Джанера на имя Арагона. Джефф рассказал о том, что после освобождения Криса из Тафт, он познакомил его с суперхакером по имени Макс Батлер. Проводившего допрос агента больше интересовала схема мошенничества с недвижимостью и на тему взлома он больше вопросов не задал.

Теперь Муларски и его конкуренты из Тайной службы знали имя. Показания Джанноне его подтверждали. Iceman рассказывал Джианноне, что его подозревали в

хищении исходных кодов Half-Life 2. Муларски запустил новый поиск и нашел ордеры на обыск по этому делу, и их оказалось всего два: против Криса Тошока и против Макса Рэя Батлера.

Личность Iceman‘а была спрятана в правительственных компьютерах всё это время. Джианноне помог агентам эту информацию найти.

Однако доказать личность Iceman‘а оказалось сложнее, чем установить. У федералов было достаточно данных для составления ордера, но они не знали расположения убежища Макса. Хуже того - Джианноне подсказал, что Iceman использует DriveCrypt. Это означало, что даже если они выяснят адрес, им не удастся извлечь никаких улик с жестких дисков. Они бы вынесли дверь в дом Макса, и уже через сутки он бы вышел из зала суда, отпущенный под залог или под роспись. А потом, воспользовавшись международной сетью по изготовлению поддельных документов, Макс мог испариться, и никто ничего бы о нём больше не услышал.

Прежде чем делать следующий шаг, им надо было всё тщательно обдумать. Муларски решил, что ключом был Крис Арагон. Благодаря Нормингтону они знали всё о денежных переводах и схеме мошенничества с недвижимостью, на которых он заработал пятью годами ранее. Если надавить этим на Арагона, его можно было вынудить к сотрудничеству против Макса.

В это время ничего не подозревающий Макс под ником Aphex продолжал своё круглосуточное управление Carders Market. Не то, чтобы новый ник кого-то обдурил. Он не сдержался и, так же как Iceman, стал поливать грязью руководителей DarkMarket и распространять найденные им доказательства против Master Splyntr. Его поражало, что так много людей ему не верят. «DarkMarket разработали и содержали люди из NCFTA и ФБР, в конце концов!»

Th3C0rrupted0ne поддержал Макса и отказался от своего статуса на DarkMarket чтобы администрировать форум Макса, посвящая сайту по 14 часов в день. Но Макс не доверял и ему. Было хорошо известно, что C0rrupted жил в Питтсбурге, где базировался и NCFTA.

Макс придумал новую схему для выявления возможных «кротов» и опробовал её на кардере в марте, заявив, то давно сотрудничает с террористической группировкой и «мы подумываем в эти выходные прихлопнуть президента Буша». По задумке Макса, если C0rrupted был федералом, он либо стал бы отговаривать его, либо постарался разузнать у Макса все детали.

Ответ Th3C0rrupted0ne немного успокоил Макса: «Удачи с этим президентским делом. Прихлопни заодно и вице-президента, он такой же хлыщ.»

Над форумом приходилось много работать. Carders Market теперь предоставлял услуги более дюжины продавцов: DataCorporation, Bolor, Tsar Boris, Perl и RevenantShadow продавали номера кредиток и коды CVV2 к ним, добытые в США, Канаде и Британии; Yevin торговал калифорнийскими водительскими удостоверениями; Notepad предлагал проверку валидности дампов за небольшую сумму; Snake Solid перемещал дампы США и Канады; Voroshilov предлагал ворам личностей услуги поиска номера социального страхования и даты рождения по имени жертвы; DelusionNFX продавал взломанные аккаунты онлайн-банков; Illusionist занимался на Carders Market тем же, что раньше делал JiLsi: продавал, бланки официальных бумаг и изображения кредитных карт; Imagine конкурировал с EasyLivin в сделках по пластику.

Макс старался чётко всё контролировать, кто-то из кардеров даже ворчал про «военизированность». В те времена, когда он был whitehat'ом, он ценил честность, но никому не давал особого статуса, даже самым близким союзникам.

В апреле C0rrupted подготовил отзыв о качестве последних версий бланков и карт, которые продавал Крис. Качество было не ахти: к примеру, полосы для подписи были напечатаны прямо на картах, приходилось писать на них маркером. Он оценивал такое на 5 из 10, но сначала решил спросить у Макса, стоит ли вскрывать эту проблему.

«Я знаю, ты хорошо знаком с Easylivin и хотел спросить - стоит ли постить такой отзыв или это будет слишком грубо?»

«Пиши правду, я думаю. Если сможешь - приложи фотографии», - написал Макс «Мы знакомы, но правда важнее. Если его покрывать - он продолжит продавать паршивые (блин, неужели настолько паршивые?) товары, это скажется на тебе и вообще всём Carders Market».

Плохой отзыв мог ударить по карману Криса. Но когда дело доходило до качества его подпольного сайта - Макс не колебался.

Глава 32. «Торговый центр»

Крис загнал Тахо в гараж торгового центра Fashion Island на пляже Ньюпорт, припарковался и вышел со своим новым партнером, двадцати трех летним Гаем Шитрид. Они отправились к Bloomingdale с поддельными кредитками American Express в бумажниках.

Шитрид из Израиля - красавчик, играющий на гитаре, и любимчик всех девушек, которого Крис встретил, занимаясь кардингом. Он проводил махинации по скиммингу в Майами, набирая профессиональных стриптизерш, снабжая их невероятно крошечным устройством для копирования информации с магнитной карты клиентов. Когда менеджеры стриптиз клуба узнали об этом, ему пришлось в спешке покинуть город. Шитрид остановился в Калифорнии, где Крис и подобрал его, снабдив поддельными документами, арендованной машиной и жильем в Арчстоуне. После они отправились по магазинам.

Теперь Крис был близок, так близок, чтобы соскочить. Его жена, Клара, привнесла на eBay $780,000 чуть более чем за три года: 2609 женских сумочек, айподов, часов от Michele и одежды от Juicy Couture. У нее был человек из прислуги, работающий двадцать часов в неделю, который занимался лишь тем, что доставлял ей вещи, купленные не за свои деньги. Крис подбрасывал к этому деньги с продаж пластика и новинок на кардерском рынке - область, не затронутая придирчивыми проверками Th3C0rrupted0ne.

Он чувствовал, что Макс не придерживался того самого плана «Whiz List»: набрать круглую сумму и свалить. В конце концов, он понял, что тот и не собирался уходить. Ему нравилось заниматься хакерством, это все что он хотел делать. К черту его. У Криса был свой запасной план. Он вложил прибыль в предприятие для Клары, компания по производству стильной джинсовой одежды Trendsetter USA, на которую уже работало несколько штатных сотрудников в ярких приятных офисах Алисо Вьехо. В итоге, он был уверен, что это будет приносить прибыль и на сто процентов законно.

До тех пор он будет занят.

Шитрид был заядлым модником, и они уже растратили часть награбленного на мужскую одежду для него. На этот раз они были сосредоточены. Вошли в наполненный прохладным воздухом Bloomingdale и пробежались по рядам с женскими сумочками, которые находились на небольших полочках вдоль стены под отдельными лампами, словно музейные экспонаты. Каждый прихватил по несколько

образцов, и они отправились на кассу. После проведения кредитных карт по нескольку раз они направились к двери с сумочками на сумму $13,000 в руках.

Крис нарушил собственные правила, войдя в магазин собственноручно, ведь его шайка быстро оскудела. Нэнси, которая помогала обустроить новый безопасный дом для Макса, переехала в Атланту, лишь изредка снимая деньги. Лиз становилась параноиком, постоянно обвиняя Криса, что тот ее кинул. Ее недовольство обосновывалось в мелочных ведомостях, написанных от руки, складывавшихся в сумму, которую Крис был ей должен за каждое их появление в магазине: $1,918 с поездки в Лас-Вегас, $674 за айподы и GPS системы, $525 за 4 сумочки стоимостью $1,750. В графе «Выплачено мне» везде красовались нули. Между тем, его новобранец – Сара, уклонялась от дорогостоящих вещей, хотя все еще была пригодна для некоторых поручений. На день Святого Валентина она купила подарки для девушки и жены Криса.

Из-за спроса на продажу, попыток начать легальный бизнес и вернуть к жизни свою шайку, Крису казалось намного более разумным платить другим за производство пластика. Он встретил Фредерика Виго на UBuyWeRush. Виго искал способы выплатить $100,000 мексиканской мафии, после того как согласился на эту сумму за импорт контрабанды хвойника из Китая, которая была перехвачена на границе. Крис нашел для него работу. Оборудование для подделок было перемещено из чайного домика в офис Виго в Нортридже, и один из подельников Криса ездил к нему пару раз в неделю чтобы забрать свежую партию новоиспеченных кредитных карт, выплачивая 10$ за каждую.

Крис и Гай покинули Bloomingdale и неспешным темпом подходили к машине. Крис открыл багажник и положил покупки среди дюжины однотонных коричневых пакетов из торгового центра, наваливавшихся друг на друга. Каждый был полон кошельков, часов и немного мужской одеждой. Закрыл багажник и сел в машину, обдумывая следующее место, куда они могли бы направиться.

Они все еще обсуждали это, когда патрульная машина полицейских заехала на стоянку. Остановившись рядом с ними, из нее вышло два офицера в форме из полицейского департамента пляжа Ньюпорт.

Сердце ушло в пятки. Еще один арест.

Полицейские отвезли их в участок, который находился далее по дороге от торгового центра, обыскали машину, где обнаружили 70 кредитных карт и немного экстази и ксанакса. После снятия отпечатков Криса сопроводили в комнату для дознания, где детектив Боб Уотс зачитал ему права и отдал на подпись.

Крис подписал и начал ту же самую историю, которая помогла ему выбраться из

серьезных неприятностей в Сан-Франциско несколькими годами ранее. Он украдкой подтвердил своё имя и признал с заметной досадой использование поддельных карт в Bloomingdale и еще кое-где. Рассказал, что это была целая организация. Он работал в сфере залога недвижимости и сильно пострадал, когда рынок недвижимости обвалился. Тогда он и был нанят распространять кредитки за небольшой процент главой Калифорнийской бандой кардеров и являлся лишь перевозчиком.

Такой расклад являлся знакомым Уотсу, который не раз ловил мелких шестерок, занимавшихся обналичкой. Это объясняло непрофессиональный налет в Bloomigdale, собравший дамских сумочек на тысячи долларов за раз. Охрана этого центра не хотела оскорблять посетителей поэтому, когда в магазине появлялись подозрительные личности, они обычно звонили Уотсу или его партнерам, которые устраивали аккуратные проверки, останавливая машины под предлогом нарушения прав дорожного движения чтобы проверить подозреваемых вне магазина. Если оказывались невиновными, они и заподозрить не могли, что это работники магазина вызвали полицейских. Поведение Шитрида и Криса, однако, было вопиющим настолько, что у сотрудников магазина не было никаких сомнений. Охрана вызвала полицию напрямую, чтобы не дать этим лицам покинуть парковочное место.

Однако Уотс не купился на историю Криса Арагона о его тяжелой судьбе. Он был детективом всего восемь месяцев, но полицейским уже семь лет. Первая вещь, которую он сделал, когда привели Арагона – пробил его по базе и выяснил, что его нелегальная деятельность брала свое начало еще в семидесятых, и, технически, он находился на условном сроке с его последнего ареста в Сан-Франциско за подделку кредитных карт.

Он полагал, что главарь сейчас сидит в его камере. Он в спешке добился ордера на обыск и присоединился к другим детективам и полицейским, которые выехали по единственному адресу, который был найден по Крису – Trendsetter USA. Один взгляд на озадаченные лица сотрудников фирмы, во время вскрытия показал Уотсу, что они невиновны. После опроса один из рабочих указал, что их босс, Клара, в главном здании вела дела с eBay.

Уотс вскрыл хранилища и изъял содержимое: 31 женская сумка, 12 новых цифровых камер Canon PowerShot, несколько GPS навигаторов TomTom, органайзеров Palm и айподы, все в запечатанных коробках.

Клара вошла в офис в середине обыска и была тут же арестована. В ее сумочке Уотс нашел несколько коммунальных счетов по адресу на пляже Капистрано, все на разные имена. Она неохотно созналась, что живет там и была сильно разочарована, когда Уотс сообщил, что это следующая его остановка.

С ключами от дома Клары и новым ордером на обыск детективы подъехали к дому Арагона и начали поиски. В домашнем офисе Криса они нашли открытый сейф в чулане. Внутри было два пронумерованных пластиковых чехла с поддельными картами. В комнате было еще больше карт, связанных резинками и спрятанных в тумбочке. MSR206 находился на полке в общей комнате, а в прилегающем гараже, рядом с тренажером, лежала коробка с сумочками.

Помимо кухни и ванных единственным местом без улик оставалась спальня мальчишек. Лишь две двуспальные кровати бок о бок и несколько мягких зверей и игрушек.

На все разговоры Криса про то, что мошенничество с кредитными картами является преступлением без жертв, он не учел двух наиболее уязвимых. Им было четыре и семь лет, и их папа не вернулся домой.

Глава 33. «Стратегия выхода»

«Это федералы» - сказал Макс, указывая на седан следовавший за ним по улице. Чарити скептически относилась к фордам. Американские машины были лишь одной из многих вещей, тревоживших Макса в эти дни.

Прошли недели с момента ареста Криса, и чтения обзоров прессы из округа Оранж, Максу не давало покоя понять, сколько улик нашла полиция в доме Арагона. Используя платежные чеки как дорожную карту, копы окружали всю команду обнальщиков; даже Маркуса, карманного садовода Криса, он же мальчик на побегушках, был пойман с фермой гидропоники, которую он растил у себя дома в Арчстоне. После двух недель охоты полиция накрыла производство кредитных карт Криса в офисе Федерико Виго в долине, арестовала Виго и захватили контрафактные детали. Крис находился под залогом в миллион долларов.

Вся операция разбиралась по частям. Они это называли, возможно, самым крупным кольцом поиска воров в истории округа Оранж.

«Черт, я предполагаю, какие записи он делал обо всем этом» - написал Макс позже The3C0rrupted0ne. «Я имею в виду, если он был достаточно небрежен, чтобы держать оборудование у себя дома.»

Макс уже уничтожил его предоплаченный сотовый и произвел блокировку аккаунта партнера в Carders Market. Это были обычные мерам предосторожности, он в не заботился об этом в первый раз; в конце концов, это был обычный случай. Крис был пойман с поличным в W, и в этот раз ушел с испытательным сроком.

Но через недели Крис оставался в тюрьме, Макс начал волноваться. Он замечал странные автомобили, припаркованные на улице вагончик службы контроля за животными вызвал подозрения, он достал фонарик, чтобы посмотреть в окна. Затем агент ФБР в Сан-Франциско неожиданно вызвал его, чтобы узнать о давно умерший базе данных паукообразных. Макс решил сделать веревочную лестницу; и держал ее у дальнего окна квартиры, делимой с Чарити, на случай если ему нужно будет экстренно уходить. Временами он останавливался, чтобы подумать о своей свободе - вот он здесь, наслаждается жизнью, хакерством, в то время как Крис находится за решеткой в округе Оранж.

Макс взял из желтых страниц случайного адвоката по уголовным делам, из Сан-Франциско, вошел к нему в офис и передал кучу наличных; он хотел, чтобы адвокат отправился в Южную Калифорнию для проверки Криса и посмотрел, что он может

сделать. Адвокат сказал, что возьмется за дело, но Макс никогда больше о нем не слышал.

Именно тогда Макс узнал о аресте Джаннона из новостной статьи о жизни Бретта Джонсона, как информатора. Макс потерял след Джаннона и всех его взломов, Макс никогда не думал о проверке имен своего окружения через публичные базы на федеральном сайте суда. Новость о том, что Джаннон проиграл судебное разбирательство его беспокоило.

«Из всех крыс и стукачей, кусков дерьма и ублюдков, Джаннон был ближе всех к сдаче меня федералам» - признался он в личном сообщении администраторам форума Carder Market. «Мелкий недоумок мог помочь федералам приблизиться ко мне».

Макс был вынужден покинуть Fox Plaza, скрывая свое оборудование дома, пока на создаст новое прибежище. Позже, 7 Июня он взял ключи от Oakwood Geary, другой корпоративной квартиры, в здании из блестящего мрамора в Tenderloin. В этот раз он был «Даниэлем Ченсом», просто еще один программным фантомом, перемещенным в Bay Area. Настоящий Ченс был 50 летним бородачом, в то время как Макс был чисто выбрит и имел длинные волосы, но поддельных прав и денежного перевода было достаточно для заселения.

Следующим вечером Макс арендовал красный мустанг в соседнем прокате ZipCar и упаковал в него компьютерные комплектующие. При всей своей паранойе, он не заметил агентов секретной службы, сидящих у него на хвосте по дороге в Oakwood, и наблюдающих с улицы, как он заезжает в свое новое убежище.

Прошел месяц. Макс вскочил на постель посреди ночи и уставился в темноту квартиры. Это просто была Чарити; Она забралась к нему в постель, пытаясь не разбудить. Нервозность увеличивалась с каждым днем.

«Милый ты не можешь больше продолжать так жить» - промурчала Чарити. «Ты этого не осознаешь, а я осознаю. Я это вижу. Ты умственно выжат. Ты не фокусируешься на том кто ты и что ты делаешь.» «Ты права» - сказал он. «Всё»

Уже достаточно времени прошло с момента его последнего тюремного срока. Может он смог бы снова найти честную работу. NightFox уже предлагал ему законную работу в Канаде, но он отказался. Он не мог заставить себя уйти от Чарити. Он рассматривал возможность брака, обыграть идею с завлечением ее на отдых в Лас-Вегас и там сделать предложение. Она была яростно независимой, но она не могла жаловаться на то что ей не хватает пространства.

Настало время для возвращения Макса Вижена в качестве white hat. Все было

официально. Он приехал в суд Сан-Франциско и заполнил необходимые документы. Уже 14 Августа судья одобрил правовую смену имени с Макса Батлера на Макса Рей Вижена. Он уже имел идею для нового сайта, которые вернул бы его обратно на white hat сцену: систему для раскрытия и управления 0day уязвимостями. Он мог наполнить его информацией о дырах в безопасности, он был причастен к андеграунду и мог переносить сплойты в мир white hat, как Чарли переносил полный чемодан государственных тайн.

После всей этой работы по созданию Carders Market, лучшего форума в англоязычном мире, он не мог просто забросить его.

Макс вернулся в свое убежище. Шел август, вернулась жара, температура на улице превышала 32 градуса Цельсия и еще выше в его студии. Процессор угрожал перегреться и сгореть. Он повернулся к вентиляторам, сел за клавиатуру и начал работать переключившись на личности Digits и Aphex.

Он вошел на Carders Market и от имени Digits оставил сообщение, что передает устройства для создания дампов одному из администраторов с ником Unauthorized. Затем от имени Aphex, он сообщил что уходит из кардинга и продает Carding Market. Он оставил сообщение повисеть несколько минут и выключил сайт. Когда он снова его включил, Achilous, один из администраторов в Канаде, уже стал смотрящим. Макс создал новую, основную запись для себя «Admin» чтобы помочь новому вору в законе от Carder Market в переходный период.

Он продолжал работать над стратегией отхода от дел, когда личное сообщение появилось на экране. Это был Silo, Канадский кардер, который всегда пытался безуспешно взломать Макса. Макс отследил его и идентифицировал как Ллойда Лиска в Британской Колумбии. Он подозревал, что Лиск информатор.

Сообщение было странным, длинное предложение о глупых ошибках новичков. Но Silo спрятал внутри второе сообщение, состоящее из девяти заглавных букв.

Они соединялись в «MAX VISION.»

Просто предположение, подумал Макс. Silo не может ничего знать.

Это было просто предположение.

• • •

Днем позже того как Макс объявил о своем отстранении, агент секретной службы Мелиса Маккензи и федеральный прокурор из Питтсбурга прилетели в Калифорнию, чтобы связать некоторые концы. Расследование было почти закончено. Секретная служба получила контактный email адрес Digits‘a из отдела

полиции Ванкувера - сподручных Silo.

Макс использовал электронную почту Канадского провайдера Hushmail, который предоставлял высокий уровень безопасности и шифрования, используя Java аплет, который расшифровывал пользовательские сообщения прямо на их PC, вместо серверов компании.

В теории, место расшифровки сообщений гарантирует, что даже Hushmail не сможет получить доступ к секретному ключу или входящим сообщениям пользователя. Компания открыто продает услугу, как способ обойти наблюдение ФБР.

Но Hushmail, так же как и e-gold, был очередным сервисом, дружественным к криминалу, и находился под разработкой спецслужб. Агентства США и Канады получили специальный ордер от верховного суда Британской Колумбии, который заставил представителей Hushmail саботировать собственную систему и скомпрометировать ключи шифрования отдельных целей. Теперь у федералов была электронная почта Макса.

В то же время агентство нашло Ти, живущую в Berkley на испытательном сроке. Оказалось, что она была поймана на использовании подарочной карты Арагона в Apple Store Эвервиля, за месяц до этого. Это было тренировочное задание для одного из новых рекрутов Криса, но Ти никогда раньше не обналичивала, и когда она добавила Power Book в ее Ipod заказ, ее арестовали вместе с новеньким стажером. Стремясь избежать больших проблем она рассказала секретной службе все, что знала.

Между тем секретная служба начала отдельно физически наблюдать за Максом. От Werner Janer’s раскрылось для Mularski что девушку Макса зовут Charity Majors. Публичные записи выдали ее адрес, а анализ банковской выписки показал, что у нее был совместный с Максом счет. Секретная служба вычислила дом и в итоге села на хвост Максу в Oakwood Geary.

Электронное наблюдение подтвердило, что Макс действовал из Oakwood. ФБР получило в суде секретный ордер, разрешающий электронную слежку за подключениями по IP к ложному Carder Market включенному на хостинге в США- современный способ записи автомобильных номеров за пределами города. Несколько трасировок вернулись к клиентам подключенных в этом же доме и использующих Wi-Fi.

За две недели до этого, девушка, агент секретной службы, под видом горничной проехала на лифте, вместе с Максом и увидела как он открывает номер 409. Номер комнаты был последним кусочком информации, который был необходим.

Была еще одна остановка перед началом движения: Окружная мужская тюрьма Orange County, мрачное отдаленное место на равнине, выжженный солнцем центр Santa Ana, Калифорния. Маккензи и федеральный прокурор Люк Дембоски посетили комнату допросов, чтобы встретиться с Крисом Арагоном.

Крис был последним задержанным в команде округа Оранж. Клара и шестеро членов команды получили обвинительный приговоры от шести месяцев до семи лет в тюрьме. Клара получила два года и восемь месяцев. Мама Криса присматривала за двумя мальчиками.

После завершения подготовки Маккензи и Дембоски приступили к делу. Они не могли ничего поделать с делом Криса, но если бы он сотрудничал, то получил бы письмо от правительства США, подтверждающее помощь федеральному прокурору. Это может повлиять на решение судьи во время вынесения приговора. Это было все, что они могли сделать.

Маккензи показывал Крису ряд фотографий и спрашивал, узнает ли он кого-нибудь. Ситуация Криса была мрачной. С его ограблением банка и контрабандой наркотиков, он мог попасть под закон «трех ошибок» Калифорнии. Это означало обязательный срок в двадцать пять лет. Крис выбрал фото Макса. Затем он рассказал историю перехода Макса Вижена на темную сторону.

• • •

В среду, 5 сентября 2007 года, Макс высадил Чарити в почтовое отделение с поручением и направил такси в магазин CompUSA даунтауна на Маркет стрит. Он выбрал новый вентилятор для своего процессора, вернулся в квартиру, разделся и завалился на кровать посреди кучи белья. Он провалился в глубокий сон.

Макс завязал с хакингом, но еще не закончил со второй жизнью, после пяти лет отношений и авантюр он не мог бросить все за ночь. Он спал, пока около двух ночи не ударили в дверь. Затем дверь вынесли и полдюжины агентов ворвались в комнату размахивая оружиям и выкрикивая приказы. Макс вскочил и закричал.

«Держи руки так, чтобы я мог их видеть!» — кричал агент. «Лежать!». Агент встал между Максом и его компьютером. Макс часто размышлял, что в случае нападения он успеет допрыгнуть до сервера и успеет включить грозную надежную защиту. Теперь, когда все это происходит, он понял, что нырнуть до компьютера не вариант, если он не хочет чтобы его расстреляли.

Самообладание вернулось к Максу. Выключенный или нет его компьютер был заблокировал и шифрование было довольно серьезным. Он немного успокоился,

агенты попросили его одеться и в наручниках повели по коридору.

По пути мимо прошла команда из трех человек, которая ждала пока секретная служба проверит убежище Макса. Они были федералами из Carnegie Mellon University’s Computer Emergency Response Team, и пришли для взлома защиты Макса.

Это был первый случай, когда сотрудники CERT участвовали в захвате, но обстоятельства были особыми. Крис Аргон использовал полное шифрование диска DriveCrypt, которое использовал Макс и ни агенты секретной службы ни CERT не смогли ничего восстановить. Полное шифрование диска держит весь диск зашифрованным всегда: все файлы, имена файлов, операционную систему, ПО, структуру директорий - ключ к тому чем занимается пользователь. Без ключа дешифрования диск можно использовать как фрисби.

Ключ полного шифрования диска можно достать пока компьютер запущен. В этой ситуации диск все еще оставался полностью зашифрованным, но ключ шифрования хранится в памяти, чтобы программы могли шифровать и дешифровывать данные с диска налету. Стук в дверь должен был отвлечь Макса от своих машин; если бы он выключил их до того как секретная служба защелкнет наручники, то даже CERT не сможет ничего сделать — содержимое оперативной памяти уже испарится. Но Макс был застигнут врасплох и сервера все еще работали.

CERT провели последние две недели разыгрывая различные сценарии того с чем они могут столкнуться в убежище Макса. Теперь командир имел следующий расклад: к серверу Макса подключено проводами полдюжины жестких дисков. Два диска были обесточены по вине агентов, запнувшихся об кабель, валяющийся на полу, но сервер все еще работал и это было важно.

В то время как прожектора секретной службы освещали загроможденную квартиру Макса, эксперты-криминалисты подъехали на машинах и начали свою работу, использую ПО для снятия дампов оперативной памяти на внешнее хранилище.

Дальше по коридору Макс следовал за федералами, в их апартаменты.

Два агента за ним приглядывали. Макс будет допрошен позже. Сейчас просто сидели с ним, болтая между собой. Агент секретной службы был из местного отделения в Сан-Франциско; он спрашивал своего коллегу из ФБР, где тот работал.

«Я из Питтсбурга,» ответил Кейт Муларски. Макс оглянулся, чтобы посмотреть на Master Splyntr. Сомнений в том кто выиграл в войне кардеров не было.

Агент секретной службы ликовала после ареста. «Я мечтала о тебе», сказала агент Мелисса Маккензи по дороге в отделение. И увидев поднятую бровь добавила: «Я имею ввиду Iceman, не Вас лично».

Два местных агента были направлены в дом Чарити. Они рассказали ей что произошло и взяли в центр, чтобы попрощаться с Максом. «Прости» — сказал Макс, когда она вошла, — «ты была права».

Макс разговорился с агентами из местного отдела, пытаясь выяснить за что его задержали и насколько велика беда. Некоторые из них удивились приветливости и дружелюбию. Макс не был черствым, как они ожидали от вора в законе, за которым охотились в течении года.

По дороге в тюрьму Маккензи наконец выразила недоумение. Похоже вы хороший парень, сказала она, все что сейчас происходит - все для вашего блага. «Но у меня есть один вопрос… Почему вы нас ненавидите?»

Макс был безмолвен. Он никогда не ненавидел секретную службу, ФБР или даже информаторов на Carder Market. Вот Iceman ненавидел. Но Iceman никогда не был реален; он был обликом, личностью, которую Макс одевал как костюм, в сети. Макс Вижен никогда никого в жизни не ненавидел.

«Голодные Программисты» были первыми, кто услышал новости о повторном аресте Макса. Тим Спенсер предложил отпустить Макса под залог. Под обеспечение он имел 20 акров земли в штате Айдахо, как свою мечту после ухода от дел. Когда Тим услышал выдвигаемые обвинения против старого друга, он заколебался. А что если он не знал Макса вообще?

Момент сомнения прошел и он подписал прошение. Мать Макса предложила заложить дом для освобождения сына. В конечном счете это не важно. Когда Макс пришел на предъявления обвинения в Сан-Хосе, федеральный судья огласил, что нужно содержать хакера под охраной до его прибытия в Питтсбург.

Правительство объявило об аресте Iceman‘а 11 сентября 2007. Новости достигли Carder Market и вызвали шквал активности. Achilous немедленно удалил все базу постов и приватных сообщений, не зная что ФБР уже владело ей.

«Я думаю SQL база уже была скомпрометирована, когда я удалял ее, но я все равно это сделал. Думаю, Aphex бы хотел этого.» Написал он. «Это форум открыт для сообщений, так что люди могли разобраться куда идти дальше. Просто будьте внимательны, особенно открывая ссылки. Пожалуйста, постарайтесь свести угрозы для всех к минимуму».

«Удачи, будьте бдительны».

Silo переключился в свой псевдоним, чтобы отметить необоснованное клеймо своего прежнего соперника, повешенное на основе новостей и работы Макса на ФБР во времена когда Макс был white hat. «Грустно видеть, что ушел хороший парень» - написал он. «Он многое принес для этого места и сцены как создатель и администратор. Многие сделали хороший деньги на нем.»

Но «скрысив однажды будешь крысой всегда» - написал он, без иронии на лице. «Вся эта доска появилась из того, что годы назад ФБР и Aphex не договорились о стукачестве… В итоге, он стал самым большим лицемерным украшением сцены.

Вернувшись за свой стол в Питтсбурге, Муларски одела черную шляпу Master Splyntr'a и присоединилась к анализу произошедшего. Агенты ФБР были полностью уверены, что Iceman не был информатором, но его альтер эго ожидало возможности воспользоваться новостями о том, что Макс работал с федералами. «Ох, а с чего я начинал?» — позлорадствовал над DarkMarket, наслаждаясь моментом. «Еще посмотрим… посмотрим… как на счет заголовка на SFGate.com? И цитаты «Экс-стукачу ФБР в Сан-Франциско предъявлено обвинение во взломе финансовых институтов.

Кто нибудь заметил что-то в этом заголовке? Ах, да, стукач ФБР. Это будет так же как и у Gollumfun и El. Не удивительно почему Iceman был для них трудной задачей, он был как они и боролся за их похвалу.

Когда Макс прибыл в Питтсбург, его общественный защитник попытался снова добиться освобождения под залог, однако судья отказал, после заявления прокурора о том, что у Макса есть огромные запасы наличных и может легко использовать свои контакты, чтобы скрыться с новым именем. Чтобы доказать, что он уже пытался уйти от федералов, они разыграли свой козырь: личные сообщения, отправленные Максом самому себе, описывающие поддельные ID, описывающие путешествие из и его передвижения в убежище. Макс отправил сообщения информатору секретной службы в Питтсбурге, который был администратором Carders market в течении целого года.

Макс совсем не удивился, что им оказался Th3C0rrupted0ne.

Глава 34. «DarkMarket»

Парень сидит на жестком полированном деревянном стуле и злобно смотрит в камеру. На фоне облезлой штукатуренной стены, он в одних трусах и держит в руках табличку. На ней большими буквами написано:

> «МОЕ НАСТОЯЩЕЕ ИМЯ — МЕРТ ОРТАЧ. Я КРЫСА, СВИНЬЯ, МЕНЯ ПОИМЕЛ CHA0.»

Появление этого фото на форуме DarkMarket в мае 2008-го заставило Муларски спешно вернуться в комнату коммуникаций NCFTA. Командному центру было бы полезно знать, что один из админов Мастера Сплинтра похитил и пытал информатора.

Cha0 был инженером в Стамбуле, он продавал для мошенников по всему миру высококачественные скиммеры и PIN-клавиатуры для банкоматов. Считыватель, установленный в банкомат, записывал информацию с магнитной ленты со всех кредиток, а фальшивая клавиатура записывала секретный PIN-код.

Его флэш-реклама на DarkMarket была классической — она начиналась с мультяшного человечка, который пробирается сквозь дом, полный денег. «Ты ли это?» — написано снизу — «Да, если ты купил считыватель и PIN-клавиатуру у Cha0.» Инструкция для новых покупателей сопровождалось улыбающейся карикатурой и самого Cha0. «Привет, меня зовут Cha0. Я разработчик скиммеров и PIN-клавиатур. Я работаю 24 часа в сутки и произвожу лучшие девайсы для скимминга. Вы сможете делать огромные деньги в этом бизнесе со мной и моей группой. Мы делаем девайсы для начинающих. Это очень просто!»

Анимированный Cha0 затем предлагает парочку полезных советов: Не устанавливайте оборудование утром, так как прохожие в это время более бдительны; Не выбирайте место, через которое в день проходит больше 250 человек; Опасайтесь городов с населением меньше 15000 — люди слишком хорошо знают, как выглядят банкоматы и могут заметить оборудование.

Мастер Сплинтр знал, что Cha0 был жженым уголовником и может применить силу, чтобы защитить свой многомиллионный бизнес, несмотря на мультяшный подход к маркетингу. И это оказалось правдой. Мерт «Kier» Ортач был частью банды Cha0 под названием Crime Enforcers, пока не сбежал на турецкую

телестанцию, чтобы настучать на Cha0. После некоторого количества интервью, он пропал. Когда же он объявился, спустя некоторое время, он рассказал о своем похищении и избиении Cha0 и его подручными.

Теперь Cha0 подтвердил эту историю, запостив фото на DarkMarket, как предупреждение остальным.

Фото оправдало давние подозрения ФБР о поднимающемся уровне насилия в компьютерном подполье. При количестве денег вложенных в подполье, стало ясно, что кардеры будут прибегать к насилию, чтобы защитить или увеличить свой источник дохода.

Макс был заключен под стражу в Огайо, и DarkMarket беспрепятственно рос. Муларски фокусировался на самых влиятельных людях и Cha0 был среди них. Турецкий киберследователь провел три месяца с Муларски бок о бок в NCFTA, чтобы вычислить производителя скиммеров.

Муларски подарил Cha0 два компьютера, тем самым сделав первый шаг в расследовании. Cha0 перенаправил посылку своим лакеям, которые были под наблюдением Турецкой Национально Полиции. Это привело к Катагэю Евьюапану (Cagatay Evyapan), электронщику с большим криминальным опытом, биография которого совпадала с биографией Cha0, которой он по секрету делился с Муларски.

Полиция посетила несколько Компаний по международной доставке и допросила их о заказах Cha0. Одна из них опознала доставку оборудования из Стамбула в Европу, и одного из участников организации как отправителя.

Это дало все улики, которые были нужны полиции. 5-го сентября пять полицейских в пуленепробиваемых жилетах ворвались в дом Cha0 на окраине Стамбула. Ворвавшись в дом, они уложили Cha0 и его приспешника на землю пригрозив оружием.

Внутри дома они нашли полноценную электролабораторию и линию производства со всеми компонентами, аккуратно разложенными по ведрам и коробкам. Где-то с десяток компьютеров работало на столах. У Cha0 было почти тоже самое оборудование для взлома карточек, как и у фабрики Криса Арагона. Те же огромные коробки, в которых лежали тысячи считывателей и PIN-клавиатур, ожидавших отправки. Записи Cha0 свидетельствовали о том, что четыре из них уже добрались до США.

Копы вывели Евьяпана в наручниках — высокого мускулистого мужчину с коротко остриженными волосами и в черной футболке с изображением смерти с косой. Лицо организованной преступности в интернете.

Cha0 был последним в списке Муларски. У DarkMarket забрали еще один козырь. Маркус Келлерер — Matrix001, был арестован в Германии в мае 2007-го, и он провел 4 месяца в тюрьме строгого режима. Ренукант «JiLsi» Сабраманиам — родившийся в Шри-Ланке житель Англии, был арестован в июле 2007-го после того, как детективы вместе с агентством по борьбе с организованной преступностью засели в интернет кафе, которое он использовал как офис, и сопоставляли его появления в кафе с его постами на DarkMarket и чатами с мастером Сплинтром. Джон «devilman» Макхью, был арестован в то же время; полиция нашла у него дома фабрику по подделыванию кредиток.

С помощью Муларски полиция также арестовала Еркана «Seagate» Финдикоглу, участника черного рынка который организовал массивную операцию по выводу денег в стиле «Король Артур», ответственную за украденные у банков 2 миллиона долларов. Им удалось вернуть один миллион после его ареста. Двадцать семь участников организации Seagate‘а были также арестованы в Турции, а ФБР арестовала шесть его выводчиков в Соединенных Штатах.

Теперь, когда Cha0 и Seagate сидели за решеткой, работа Муларски была завершена. DarkMarket за два года «принес» Муларски 56 арестов в 4х странах. Во вторник,16 сентября 2008 года, он опубликовал пост, объявлявший о закрытии DarkMarket. Как дань истории и культуре кардинга, агент ФБР позаимствовал легендарное сообщение Короля Артура о закрытии Планеты Кардинга несколько лет назад:

> «Добрый день, дорогие и уважаемые участники форума» — начал он — «настало время сообщить вам плохие новости — форум будет закрыт. Да, реально закрыт. За последний год мы потеряли огромное количество админов на форумах: Iceman на Carders Market, JiLsi и Matrix001 исчезли, вот теперь и Cha0 на DM. Становится ясно, что этот форум, проживший почти 3 года, начал привлекать слишком много внимания мировых спецслужб.
>
> Я предпочту уйти как Король Артур, а не как Айсмэн. Айсмэн решил просто сменить ник на Aphex, и продолжил управлять CM. Король Артур просто закрыл Carder Planet и исчез в ночи. История показала, что Айсмэн сделал огромную ошибку. Я не повторю ее.»

Муларски планировал поддерживать легенду Мастера Сплинтра. Это была отличная легенда, которая могла пригодиться для будущих расследований. Но это не случилось. Спустя неделю после закрытия DarkMarket, репортер Sudwestrundfunk, юго-западного германского публичного радио получил судебные

документы по делу Matrix001, которые похоронили легенду Муларски. Американская пресса очень быстро подхватила историю. Теперь 2500 участников DarkMarket знали, что они делали дело на подставном сайте и что Айсмэн был прав все это время.

Спустя три дня после провала легенды, Муларски нашел сообщение ICQ, адресованное Мастеру Сплинтру. Оно было от TheUnknown, одного из подозреваемых, которому удалось скрыться от полиции. «Ты хуев кусок говна. Ублюдок. Думал ты меня поймаешь? Ха-ха. Долбаный новичок. Ты даже близко ко мне не подошел.»

«Если хочешь сдаться, дай мне знать.» — ответил Муларски. — «Это будет легче, чем всю жизнь оглядываться.»

TheUnknown сдался неделю спустя.

Муларски вздохнул с облегчением, узнав что он раскрыт. Два года подряд ноутбук был его постоянным спутником — даже в отпуске он был в сети, разговаривая с мошенниками. Ему иногда это доставляло удовольствие — строить отношения с подозреваемыми, дразнить и насмехаться над ними. Мастер Сплинтр мог говорить такие вещи преступникам, которые не смог сказать ни один уважаемый агент ФБР.

Муларски стремился вернуть свою привычную жизнь назад, для этого требовалось время. Даже спустя месяц после закрытия DarkMarket, он все еще боролся с беспокойством. У Муларски была еще одна цель. Перестать быть мастером Сплинтром.

Глава 35. «Приговор»

Макс возвышался над судебными приставами, доставившими его в зал Питсбургского суда для вынесения приговора. Он был одет в плохо сидящую на нем оранжевую тюремную униформу, волосы коротко и четко острижены. Конвой снял наручники, и он сел за стол для ответчика рядом с государственным защитником. В зале на одной стороне переговаривались между собой с полдюжины репортеров, на другой - такое же количество федералов. Позади них длинные деревянные скамьи были почти пусты: ни друзей, ни членов семьи, ни Черити - она уже сказала Максу, что не станет его дожидаться.

Это было 12 февраля 2010 года, два с половиной года спустя после его ареста на конспиративной квартире. Первый месяц под стражей Макс провел в окружной тюрьме Санта-Клары, каждый день подолгу разговаривая по телефону с Черити. Эти разговоры были более близкими, чем все их общение в то время, когда он был поглощен своими преступными делами. Потом приставы посадили его на самолет и перевезли в место временного содержания в Огайо. Там Макс уже смирился со своим заключением, израсходовав весь лицемерный гнев, поддерживавший его до конца предыдущих сроков заключения. Он нашел здесь новых друзей — таких же гиков. Она стали играть в Dungeons and Dragons.

К концу года у Макса больше не осталось секретов. Всего две недели потребовалось следователям из CERT, чтобы найти ключ шифрования в образе оперативной памяти, снятом с его компьютера. На одном из судебных заседаний обвинитель Люк Дембоски протянул адвокату Макса листок бумаги, где была написана его парольная фраза: «!!Один человек может многое!».

Годами Макс использовал зашифрованный жесткий диск как расширение своего мозга, сохраняя все, что он находил и все, что делал. То, что федералы заполучили все это, было конечно пагубным для его будущего с точки зрения закона, но мало того, это было как вторжение в его личность. Власти залезли ему в голову, читая мысли и воспоминания. Вернувшись в камеру после того заседания, он рыдал в подушку.

Они получили все: пять терабайт хакерских инструментов, фишинговых писем, досье, которые он собирал на своих сетевых друзей и врагов, заметок о его делах и интересах, и данные 1,8 миллиона кредитных карт из более, чем тысячи банков. Власти разобрали их все: 1,1 миллион карт Макс украл из POS систем. Остальные были в основном от других кардеров, которых Макс взломал.

Если измерить их длиной магнитных полос, получалось восемь миль, и федералы были готовы привлечь его к ответу за каждый дюйм. Власти тайно привезли Криса на несколько недель в Питсбург для разбора действий. Компании-владельцы карт подсчитали объем фрода по картам Макса и пришли к ошеломляющей цифре: 86,4 миллиона долларов убытков.

Прибыль же Макса была намного меньше: Макс рассказал властям, что заработал не больше миллиона долларов на своих махинациях и большую их часть он спустил на аренду жилья, еду, такси и гаджеты. В кошельке WebMoney Макса обнаружили около $80,000. Но Федеральные директивы по назначению наказаний за кражу основываются на ущербе потерпевших, а не на выгоде злоумышленников. Так что Максу светило ответить за суммы, снятые и Крисом, и кардерами, купившими дампы у Digits and Generous, и возможно даже за фрод, совершенный теми кардерами, которых Макс сам взломал. Если подбить итог по всему «послужному списку», то 86 миллионов выливались в срок от тридцати лет до пожизненного, без права на досрочное освобождение.

Перед лицом перспективы провести в тюрьме десятилетия Макс начал сотрудничать со следствием. Муларски забирал хакера на долгие сеансы разбора его преступлений. На одной из них, после того, как операция против DarkMarket появилась в прессе, Макс извинился перед Муларски за свои попытки подставить Master Splyntr. Муларски услышал искренность в словах давнего врага, и извинения были приняты. После года переговоров, адвокат Макса и сторона обвинения сошлись на одной цифре - совместной просьбе суду назначить тринадцать лет. В июле 2009 года Макс признал свою вину.

Но эта сделка не была обязательной для суда. Теоретически, Макса могли как отпустить из зала суда, так и приговорить к пожизненному сроку, или же назначить ему что угодно между этими крайностями. Накануне дня приговора Макс набрал четыре страницы письма к Морису Кохилу, семидесятилетнему судье, назначенному президентом Фордом, который стал юристом еще до того, как Макс родился на свет.

«Я не уверен, что дальнейшее заключение в тюрьме кому-либо поможет в моем случае.» — писал Макс. «Я не думаю, что это необходимо, потому что все, что я хочу — это помочь. Я не согласен с бездумными оценками из Директив по назначению наказаний. К сожалению, мне светит настолько ужасный приговор, что даже 13 лет кажутся сравнительно «неплохим» сроком. Но я вас уверяю, что и это лишнее, это как стегать мертвую лошадь. Тем не менее, я собираюсь наилучшим образом использовать время, оставшееся мне на этой земле, будь то в тюрьме или где-то еще.»

Он продолжал: «Я сожалею о многом, но, думаю, основной моей ошибкой было то, что я потерял связь с той ответственностью и теми обязательствами, которые налагаются на меня как на члена общества. Мой друг как-то посоветовал мне вести себя так, как будто все всегда могут видеть, что я делаю. Это хороший способ избежать противозаконного поведения; но, похоже, я не проникся им, так как будучи невидимым, я забыл об этом совете. Теперь я знаю, что мы не можем быть невидимыми, опасно так думать.»

Макс с напускным спокойствием наблюдал, как его адвокат совещается с обвинением о каких-то последних деталях, а судебные служащие выполняют свои обязанности перед заседанием, проверяют микрофоны и перекладывают бумаги. В десять-тридцать утра дверь кабинета судьи открылась. «Всем встать!»

Судья Кохил занял свое место. Суховатый мужчина с коротко остриженной белоснежной бородой, он оглядел зал суда сквозь круглые очки и объявил вынесение приговора Максу Батлеру, под этим именем Макс фигурировал в обвинении. Он зачитал для протокола Директивы о назначении наказаний, от тридцати лет до пожизненного, затем стал слушать, как обвинитель Дембоски излагал свои доводы о снисхождении. Макс оказал существенную помощь властям, говорил он, и заслуживает более мягкого приговора, чем предписано директивами.

Дальнейшее действо было скорее похоже на присуждение наград, а не наказания; когда адвокат Макса, обвинитель и сам судья по очереди превозносили его компьютерные таланты и бесспорное раскаяние. «Он на редкость блестящий компьютерный эксперт-самоучка» - говорил федеральный государственный защитник Майкл Новара, хотя он и организовал «взломы систем безопасности грандиозного масштаба».

Дембоски, эксперт по компьютерным преступлениям и заслуженный работник Прокуратуры с семилетним стажем, назвал Макса «чрезвычайно ярким и талантливым». Он присутствовал на некоторых из сессий разбора действий Макса, и вместе с практически всеми, кто знал Макса в реальной жизни, проникся к хакеру симпатией. «Он оптимистичен, почти наивен в своем взгляде на мир» - сказал он. Сотрудничество Макса, добавил он, стало причиной, по которой они просят только тринадцать лет вместо «астрономического» срока. «Я уверен, что он очень сожалеет.»

Макс не много смог добавить к сказанному. «Я изменился» — сказал он. Хакерство больше не привлекало его. Он предложил судье Кохилу задеть ему любые вопросы. Кохилу этого не требовалось. Судья сказал, что он был впечатлен письмом Макса, а также письмами, написанными Черити, Тимом Спенсером, матерью, отцом и сестрой Макса. Он был удовлетворен тем, что Макс раскаялся. Я

не думаю, что должен прочесть вам лекцию о тех проблемах, которые вы создали своим жертвам.

Кохил уже написал приговор. Он громко зачитал его. Тринадцать лет тюрьмы. Также Макс обязан возместить 27,5 миллионов долларов убытков, это стоимость перевыпуска 1,1 миллиона банковских карт, которые Макс украл через POS терминалы. После своего освобождения он должен находиться под надзором еще пять лет, в течение которых ему разрешается пользоваться Интернетом только в служебных или образовательных целях.

«Удачи» — сказал он Максу.

Макс встал, с безразличным лицом, и дал приставу застегнуть сзади наручники и увести его через дверь на задней стороне зала суда, ведущей к камерам. С учетом уже отбытого срока и хорошего поведения он должен будет выйти в 2018 году, как раз перед Рождеством.

Впереди у него были еще девять лет тюрьмы. Это был самый долгий срок, когда-либо присужденный хакеру в США.

Глава 36. «Последствия»

К тому моменту, когда Макс Вижн был осуждён, Секретная Служба уже смогла идентифицировать загадочного американского хакера, который сделал Maksik‘а одним из крутейших кардеров мира, и готовилась его осудить, что стало бы некоторым смягчением ситуации для Макса.

Переломный момент в том деле произошёл после событий в Турции. В июле 2007-ого, турецкая полиция получила от Секретной Службы информацию, что Maksik это двадцатипятилетний Максим Ястремский, отдыхающий в Турции. Агент под прикрытием заманил его в ночной клуб в Кемере, где полиция арестовала его и изъяла ноутбук.

Полицейские обнаружили, что жёсткий диск ноута наглухо зашифрован, примерно также как и во время скрытой операции в Дубаи, годом ранее, когда копы пытались незаметно слить его содержимое. Однако проведя несколько дней в турецкой тюрьме, Maksik выдавил из себя нужный семнадцатисимвольный пароль. Полицейские сняли с диска шифрование и передали содержимое в Секретную Службу, где принялись пристально изучать данные. Наибольший интерес для них представляли логи Maksik‘а в ICQ.

Один из собеседников отличался от остальных: пользователь с UIN 201679996, по видимому, помогал Maksik‘у с атакой на сеть ресторанов Dave & Buster’s и обсуждал с ним некоторые из предыдущих высококвалифицированных взломов, которыми Maksik заявил о себе. Агенты проверили данный UIN и узнали e-mail, использованный при регистрации: soupnazi@efnet.ru.

SoupNazi это псевдоним, ставший известный агентам секретной службы ещё в 2003-м году при аресте Альберта Гонсалеса.

Гонсалес был информатором, который сдал секретной службе кардеров из Shadowcrew, заманив их в подставной VPN. Его действия привели к двадцати одному аресту в ходе операции Firewall - легендарному удару секретной службы по кардинг-сцене. За многие годы до участия Гонсалеса в Shadowcrew, его псевдонимом в IRC был SoupNazi.

Похоже, что стукач, ранее позволивший провести операцию Firewall, теперь вышел на новый уровень и стал совершать крупнейшие сетевые кражи в истории США.

Через месяц после операции Firewall Гонасалес получил разрешение переехать из Нью-Джерси обратно домой, в Майами, где он и начал второй эпизод своей хакерской карьеры. Он взял никнейм Segvec и выдавал себя за украинца под ником Mazafaka на Восточно-Европейском форуме. Под девизом «Стань Богатым или Умри Пытаясь» (название альбома 50 Cent‘a и девиз Maksik’а в Shadowcrew), Гонсалес начал серию многомиллионных киберкраж, которые коснулись десятков миллионов американцев.

Восьмого мая 2008 года федералы задержали Гонсалеса и его сторонников в США. Пытаясь смягчить приговор, Гонсалес вновь сотрудничал с агентами, сдав им ключ шифрования от собственного диска, а также информацию обо всех своих соратниках. Он признался во взломах TJX, OfficeMax, DSW, Forever 21 и сети Dave & Buster’s. Помимо этого он также признал, что помогал восточноевропейским хакерам при взломах сети магазинов Hannaford Bros., сетей 7-Eleven’s ATM network и Boston Market, а также процессинговой компании Heartland Payment Systems, из которой хакерам удалось увести около 130 миллионов карт. Это было весьма прибыльное время для хакера. В ходе расследования Гонсалес показал федералам задний двор своих родителей, где он зарыл более миллиона долларов наличными. Правительство добилось конфискации этих денег, а также спортивного BMW Гонсалеса и его огнестрельного Glock 27.

Гонсалес набирал свою команду из «нетронутого резервуара» подпольных хакеров, которых не признали на white-hat сцене. Среди них был и Джонатан “C0mrade” Джеймс. Ещё будучи подростком он взломал NASA и получил за это шесть месяцев условно, кстати, это произошло в ту же неделю, когда Макс Вижн признал себя виновным во взломах Пентагона в 2000-ом. После непродолжительной славы и нескольких интервью в популярных СМИ Джеймс предпочёл уйти за кулисы и спокойно жить в доме, который он унаследовал от своей матери, в Майами.

Затем, в 2004-ом он якобы начал работать с Гонсалесом и его помощником Кристофером Скоттом. Федералы были уверены, что Джеймс и Скотт достали первые дампы карт в хранилища Maksik’а, а также были ответственны за взлом Wi-Fi сети магазинов OfficeMax’s и кражу тысяч зашифрованных дампов и PIN. Эти двое обеспечивали Гонсалеса данными, а он договаривался с неким другим хакером на счёт их расшифровки. После этих атак, компании выпустившие украденные карты были вынуждены перевыпустить около 200 000 карт.

Из всех хакеров, Джонатан Джеймс заплатил самую высокую цену за своё преступное прошлое. После майского рейда в 2008-м, Джонатан убедился, что Секретная Служба будет пытаться повесить на него все преступления Гонсалеса, чтобы оправдать своего информатора в глазах общественности. Восемнадцатого мая

двадцатичетырёхлетний паренёк пошёл в ванну, взяв свой пистолет, и застрелился.

«Я разочаровался в нашей системе правосудия,» - писал он в своей пятистраничной посмертной записке. «Возможно, это послание и то, что я сделаю сегодня, дойдёт до сознания общественности. Как бы там ни было, я потерял контроль над ситуацией, и это единственное, что я могу сделать, чтобы всё исправить.»

В марте 2010-ого Гонсалес был приговорён к двадцати годам тюрьмы. Его соучастники получили от двух до семи лет. А тем временем в Турции Maksik был признан виновным во взломах Турецких банков и приговорён к тридцати годам заключения.

После ареста Макса, мошенники из андеграунда продолжили кидать людей. В худших случаях они использовали трояны, чтобы украсть пароли к online-банкингу жертв и перевести деньги прямо с атакуемого компьютера. Воры придумали достаточно остроумный способ для решения проблемы, беспокоившей когда-то Криса Арагона - как же, собственно, получить деньги? Они нанимали простых людей, для, якобы, «работы на дому», а сама работа заключалась в получении денег и зарплаты переводами и дальнейшей пересылке основной части денег в Восточную Европу через систему Western Union. В 2009-ом, когда данная схема впервые стала действительно массовой, банки и их клиенты потеряли около 120 миллионов долларов, а основной целью атак был малый бизнес.

Тем временем продажи дампов продолжаются и по сей день, теперь уже в основном новым поколением «поставщиков», хотя можно встретить и старые имена - Mr. BIN, Prada, Vitrium, The Thief.

Правоохранительные органы однако уверяют, что им удалось добиться неких долговременных результатов. К примеру, до сих пор не появилось ни одного известного англоязычного форума на замену Carders Market‘у и DarkMarket‘у, а восточноевропейские борды стали более закрытыми и защищёнными. Серьёзные игроки стали использовать шифрованные чат-серверы, работающие только по инвайтам. Чёрный рынок до сих пор жив, однако кардеры потеряли чувство безнаказанности, и их деятельность пропиталась паранойей и недоверием, благодаря, в основном, деятельности ФБР, Секретной Службы и содействующим им почтовым отделениям, а также их международным партнёрам.

Завеса секретности, что некогда окружала хакеров и корпорации, похоже, начала испаряться, а законодательство более не позволяло компаниям оправдываться своей собственной незащищённостью. Несколько имён компаний, пострадавших от взломов Гонсалеса, были обнародованы в ходе судебного процесса.

И наконец, укол, нанесённый Муларски DarkMarket‘у, дал понять, что федералам не обязательно идти на сделку с плохими парнями, чтобы проводить свои рейды.

Все самые подлые эпизоды в войнах компьютерного андеграунда происходили «с руки» информаторов: например Бретт «Gollumfun» Джонсон превратил операцию Секретной Службы «Рыба-Удильщик» в форменный балаган, когда начал проворачивать налоговые афёры на стороне. Альберт Гонсалес тоже был показательным примером - после операции Firewall Секретная Служба платила ему около 75000$ в год, тогда как он сам в это время проворачивал крупнейшие кражи в истории.

Взломы проведённые им уже после выхода из Shadowcrew, привели к множественным судебным тяжбам. TJX выплатила десять миллионов долларов чтобы закрыть судебные дела, возбуждённые против неё в более чем сорока странах мира и ещё 40 миллионов долларов банкам, чьи карты были скомпрометированы. Банки и кредитные организации также подали множество судебных исков против Heartland Payment Systems из-за массовых нарушений обработок транзакций. Атаки Гонсалеса пробили настоящую дыру в главном защитном бастионе всей индустрии кредитных карт: так называемый Payment Card Industry Data Security Standard, стандарт, который описывает все шаги, которые торговцы и процессинговые центры должны предпринимать для защиты данных кредитных карт. Heartland имел сертификат PCI, а Hannaford Brothers прошли сертификацию даже когда хакеры ковырялись в их системах, продолжая воровать данные.

Когда поутихла шумиха вокруг грандиозных краж Гонсалеса, начались менее масштабные, но гораздо более многочисленные атаки на различные сети ресторанов, использующие POS. Семь ресторанов в Миссисипи и Луизиане, которые подверглись взломам, обнаружили, что все они используют один и тот же POS-процессинг - Aloha POS, который, кстати, был одной из любимых мишеней Макса. Рестораны подали групповой иск против производителя и компании, которая продала им терминалы - Computer World из Луизианы, которая якобы установила на всех терминалах ПО для удалённого доступа и установила пароль «computer» на каждом из них.

Первопричиной всех этих взломов была всего лишь одна единственная дыра в безопасности, размером ровно 3.375 дюйма — магнитная полоса на кредитной карте. Это технологический анахронизм, флешбэк из эры кассет на магнитной ленте, и на сегодняшний день США практически единственная во всём мире страна, которая оставляет эту уязвимость открытой. Более сотни стран по всему миру, в Европе, Азии, даже в Канаде и Мексике уже используют или начинают использовать гораздо более защищённую систему под названием EMV, или chip-and-PIN. Вместо пассивной магнитной полосы новые карты используют микрочип

встроенный непосредственно в пластик карты, который использует алгоритм криптографического «рукопожатия» для аутентификации в POS-терминале и дальнейшей связи с процессинговым центром. Данная система не позволяет скопировать карту даже взломщику, имеющему полный доступ к линии передачи данных, поскольку последовательность используемая при «рукопожатии» меняется каждый раз.

White-hats разработали несколько атак на систему EMV, но ничего из этого не применимо на современном массовом рынке дампов. На данный момент основная брешь в новой системе это возможность проводить операции по магнитной полосе, в качестве запасного варианта для американцев, выезжающих за рубеж или туристов, посещающих Соединенные Штаты.

Американские банки и кредитные организации отказались вводить chip-and-PIN, из-за космической стоимости замены сотен тысяч POS-терминалов на новые. В конце концов, финансисты решили, что убытки от мошенников вполне приемлемы, даже если взломщики, подобные Iceman‘у, бродят по их сетям.

Эпилог

In the Orange County men's jail, Chris Aragon is lonely, feeling abandoned by his friends and torn with grief that his children are growing up without him. In October 2009, Clara filed for divorce, seeking custody of their two children. His girlfriend filed for child support.

Chris is studying the Bhagavad Gita and has a full-time job as an inmate representative, helping several hundred prisoners with legal matters, medical complaints, and issues with the jail staff. His lawyer is playing a waiting game, winning endless continuances for the criminal trial that, if he loses, still carries a twenty-five-to-life term. After Chris's story was featured in a Wired magazine article on Max, Chris was contacted by a Hollywood screenwriter and a producer, but he didn't respond. His mother suggested he get an agent.

Max was assigned to FCI Lompoc, a low-security prison an hour north of Santa Barbara, California. He hopes to use his time to get a degree in physics or math—finally completing the college education that was interrupted a decade earlier in Boise.

He's taken a mental inventory and is dismayed to find that, despite everything, he still has the same impulses that guided him into a life of hacking. "I'm not sure how to really mitigate that, except ignore it," he said in an interview from jail. "I really believe that I'm reformed. But I don't know what's going to happen later."

It might seem a curious confession—admitting that the elements of his personality that landed him in prison still remain buried deep inside. But Max's new self-awareness shows hope for real change. If one is born a hacker, no amount of prison can drive it out. No therapy, or court supervision, or prison workshop can offer reform. Max has to reform himself—learn to own his actions and channel the useful parts of his nature into something productive.

To that end, Max has volunteered to help the government during his confinement, defending U.S. networks or perhaps counterattacking foreign adversaries online. He wrote out a menu of the services he could offer in a memo headed "Why the USA Needs Max." "I could penetrate China's military networks and military contractors," he suggested. "I can hack al Qaida." He's hopeful he might do enough for the government that he could apply for a lowered sentence from his judge.

It's a long shot, and so far, the feds haven't taken him up on his offer. But a month after his sentencing, Max took a baby step in that direction. Keith Mularski arranged for Max to speak at the NCFTA for an eager audience of law enforcement officials, students,

financial and corporate security experts, and academics from Carnegie Mellon.

Mularski checked him out of jail for the appearance. And for an hour or two, Max Vision was a white hat again.